

# 美国网络安全战略与政策二十年

左晓栋 等 编译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

## 内 容 简 介

本书收录了自 1998 年至今克林顿、小布什、奥巴马和特朗普共四任总统任期内，美国政府、军方、国会和有关部门发布的主要网络安全战略、法律、规划、行政令、总统令，以及根据美国网络安全战略要求，各关键基础设施部门发布的本行业网络安全战略和规划，共计 36 篇，并以时间顺序排列。附录 I 还摘要介绍了美国重要智库战略与国际研究中心（CSIS）对特朗普政府的网络安全政策给出的建议。为了更全面地反映美国网络安全政策制定过程，本书收录的文件包括一些过程稿或征求意见稿。

考虑到篇幅等因素，本书对各行业的网络安全战略和规划进行了摘要介绍，全部详细内容可通过扫描书中给出的二维码免费阅读。

本书可供各级网络安全和信息化领导机构以及各网络安全主管部门、各关键信息基础设施主管或监管部门在制定网络安全政策时参考，也可供各类网络安全管理和技术人员在实际工作中参考，还可用作高等院校和科研机构在网络安全、国际关系等专业方向的教学或研究参考资料。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

### 图书在版编目（CIP）数据

美国网络安全战略与政策二十年 / 左晓栋等编译. —北京：电子工业出版社，2017.12

ISBN 978-7-121-33159-6

I. ①美… II. ①左… III. ①计算机网络—国家安全—国家战略—研究—美国 IV. ①D771.236  
②TP393.08

中国版本图书馆 CIP 数据核字（2017）第 316673 号

策划编辑：齐 岳

责任编辑：苏颖杰

印 刷：

装 订：

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1092 1/16 印张：49.25 字数：1261 千字

版 次：2017 年 12 月第 1 版

印 次：2017 年 12 月第 1 次印刷

定 价：298.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 [zltz@phei.com.cn](mailto:zltz@phei.com.cn)，盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

本书咨询联系方式：（010）88254473、[qiyue@phei.com.cn](mailto:qiyue@phei.com.cn)。

# 前 言

习近平总书记指出，没有网络安全就没有国家安全。中央网络安全和信息化领导小组成立以来，特别是“4·19”网络安全和信息化工作座谈会召开后，在习总书记“网络强国”战略思想指引下，我国网络安全工作进入了加速发展的崭新阶段，《网络安全法》、《国家网络空间安全战略》的出台推动网络安全顶层设计趋于完善，关键信息基础设施安全保护等重要制度相继建立，国家网络安全保障体系日益健全，维护国家空间、主权和国家安全的能力显著增强。

与此同时，网络安全形势仍十分严峻，各国在网络空间展开激烈博弈，围绕网络空间发展权、主导权、控制权的竞争愈演愈烈。知彼知己，百战不殆。做好自己的事情重要，了解别人也同样重要。加之网络安全是开放而不是封闭的，维护国家网络安全要有全球视野和开放心态，因此更有必要关注其他国家的做法。

美国全面加强网络安全工作已有二十年的历史，是值得我们关注的重点对象。1996年，美国国防授权令要求美国总统从防止战略攻击的角度向国会报告联邦政府的网络安全政策。为此，经过一系列国家安全会议的讨论，当时的美国总统克林顿发布了第63号总统决定令（PDD63）《对关键基础设施保护的政策》，从此拉开了美国以关键基础设施保护为重点的网络安全工作历史大幕。二十年间，美国历经四任总统，围绕网络安全先后发布了一系列战略、法律、规划、行政令、总统令。

在中央网络安全和信息化领导小组办公室的关心、支持和指导下，我们对美国的这些文件进行了全面回顾、翻译和研究，并编译成本书。前事不忘，后事之师。我们不但关注特朗普政府的最新网络安全政策，而且重视早期的美国网络安全战略部署，甚至是一些战略的过程稿。正是这些文件，使我们得以完整地看到美国网络安全机构演变过程和网络安全思路调整脉络，这是重要的他山之石，希望能为我国网络安全工作提供参考。

左晓栋

2017年12月





# 目 录

一、第 63 号总统决定令：克林顿政府对关键基础设施保护的政策 .....	1
1. 日益增长的潜在脆弱性 .....	2
2. 总统的意愿 .....	2
3. 国家目标 .....	2
4. 公共-私营合作联盟以减少脆弱性 .....	3
5. 方针 .....	3
6. 结构和组织 .....	4
7. 保护联邦政府的关键基础设施 .....	5
8. 任务 .....	5
9. 执行 .....	6
附录 A 结构和组织 .....	6
附录 B 其他任务 .....	9
二、保护美国的网络空间——信息系统保护国家计划 .....	11
总统的话 .....	12
国家协调员的话 .....	13
1. 美国关键基础设施面临的威胁 .....	32
2. 保护隐私与公民自由 .....	39
3. 计划的目标和范围 .....	42
4. 联邦政府关键基础设施保护计划 .....	45
5. 私营部门以及州和地方政府的关键基础设施保障框架 .....	101
附录 A 主要的联邦 CIP 官员和联系方式 .....	110
附录 B 预算趋势 .....	110
附录 C 关键基础设施保护中的联邦研发日程 .....	116
附录 D 术语表和缩略语 .....	129
三、第 13231 号行政令：信息时代的关键基础设施保护 .....	134
1. 政策 .....	135
2. 范围 .....	135

3. 设立机构·····	135
4. 进一步授权·····	135
5. 委员会职责·····	136
6. 成员·····	137
7. 主席·····	138
8. 常设委员会·····	138
9. 规划和预算·····	139
10. 总统的咨询委员会·····	140
11. 国家通信系统·····	141
12. 反情报·····	141
13. 定密权·····	141
14. 一般条款·····	141
<b>四、《保护网络空间的国家战略（草案）》的 53 个重要问题</b> ·····	<b>142</b>
译者注·····	143
第 1 级：家庭用户和小型商业机构·····	143
第 2 级：大型机构·····	143
第 3 级：国家信息基础设施部门·····	144
第 4 级：国家机构和政策·····	146
第 5 级：全球·····	147
<b>五、保护网络空间的国家战略（草案）</b> ·····	<b>148</b>
委员会主席和副主席的信·····	149
1. 介绍·····	150
2. 网络空间威胁与脆弱性：行动案例·····	153
3. 国家政策与指导原则·····	158
4. 本部战略的重点·····	162
5. 第 1 级：家庭用户和小型商业机构·····	166
6. 第 2 级：大型机构·····	170
7. 第 3 级：关键部门·····	174
8. 第 4 级：国家的优先任务·····	192
9. 第 5 级：全球·····	205
10. 建议概要·····	208
<b>六、保护网络空间的国家战略</b> ·····	<b>215</b>
1. 执行摘要·····	216
2. 介绍·····	221
3. 网络空间威胁和脆弱性·····	224
4. 国家政策与指导原则·····	229
5. 优先事务 I：国家网络空间安全响应系统·····	232

6. 优先事务II：国家网络空间安全威胁和脆弱性消减计划	237
7. 优先事务III：国家网络空间安全意识和培训计划	243
8. 优先事务IV：保护政府部门的网络空间安全	248
9. 优先事务V：国家安全和国际网络空间安全合作	252
10. 总结：前方之路	254
附录 行动与建议（A/R）概要	255
<b>七、关键基础设施和重要资产的物理保护国家战略</b>	<b>260</b>
1. 执行摘要	261
2. 介绍	268
3. 行动案例	271
4. 国家政策和指导方针	276
5. 跨部门安全优先级	283
6. 确保关键基础设施的安全	295
7. 保护国家重要资产	321
8. 总结	327
<b>八、工业界对国家战略的响应纲要（摘要）</b>	<b>329</b>
1. 目的	330
2. 背景	330
3. 介绍	330
4. 各部门面对的共同问题	331
5. 总结	334
<b>九、研发项目开发计划：通过信息安全技术实现关键基础设施保护（摘要）</b>	<b>335</b>
1. 介绍	336
2. 现状分析	338
3. 研发项目开发计划：任务及其相关关系	344
4. CIP 中的 InfoSec 技术研究领域	345
5. CIP 中的 InfoSec 运行研究领域	349
6. 总结	352
<b>十、银行与金融部门关键基础设施保障国家战略（摘要）</b>	<b>353</b>
执行摘要	354
1. 银行与金融部门透视	355
2. 关键基础设施保障战略指导	367
3. 加强基石建设	374
4. 其他考虑	380
<b>十一、信息与通信部门的关键基础设施和网络空间安全国家战略（摘要）</b>	<b>395</b>
执行摘要	396

1. 背景与范围 .....	397
2. 威胁、脆弱性与风险管理 .....	400
3. 工业界与政府的角色 .....	407
4. 展望 .....	410
<b>十二、高等教育对保护网络空间的国家战略的贡献（摘要） .....</b>	<b>412</b>
执行摘要 .....	413
1. 介绍 .....	413
2. 高教部门的网络安全工作 .....	414
3. 美国高教部门人口统计 .....	414
4. 美国高教部门的组织 .....	415
5. 网络安全与高等教育的使命 .....	416
6. 网络安全与高等教育的价值体现 .....	417
7. 高教部门的计算机和网络基础设施 .....	418
8. 回应有关国家战略的问题 .....	419
9. 网络安全行动框架 .....	420
10. 下一步行动 .....	421
11. 总结 .....	423
<b>十三、美国化学部门网络安全战略（摘要） .....</b>	<b>424</b>
执行摘要 .....	425
1. 化学部门的背景 .....	425
2. 情况分析 .....	427
3. 美国化学部门网络安全战略建议 .....	430
<b>十四、电力部门对关键基础设施保护挑战的回应（摘要） .....</b>	<b>437</b>
1. 介绍 .....	438
2. 方案概述 .....	438
3. 本行业的历史使命 .....	439
4. 电力部门行动方案的要素 .....	441
5. 总结 .....	446
<b>十五、保险部门对保护网络空间的国家战略的响应 v5.1（摘要） .....</b>	<b>447</b>
1. 保险部门简介 .....	448
2. 总结 .....	450
<b>十六、供水部门关键基础设施保护国家计划（摘要） .....</b>	<b>452</b>
1. 引言 .....	453
2. 供水部门的代表 .....	453
3. 顾问组 .....	454
4. 信息共享和分析中心 .....	454

5. 供水部门的问题·····	454
<b>十七、铁路部门关键基础设施保护国家计划（摘要）·····</b>	<b>455</b>
1. 行业概述·····	456
2. 现任部门协调员的活动·····	456
3. 铁路部门对“9·11”事件的反应·····	457
4. 恐怖主义风险分析和安全管理计划·····	458
5. 联邦政府的参与·····	459
6. 总结·····	460
<b>十八、保护新经济时代石油和天然气基础设施的安全（摘要）·····</b>	<b>461</b>
介绍·····	462
1. 新经济环境·····	462
2. 脆弱性、后果和威胁·····	465
3. 风险管理·····	470
4. 响应和恢复·····	475
5. 信息共享和部门协调·····	480
6. 有关信息共享的法律法规问题·····	485
7. 研究与开发需要·····	489
<b>十九、第 7 号国土安全总统令：关键基础设施标识、优先级和保护·····</b>	<b>491</b>
1. 目的·····	492
2. 背景·····	492
3. 定义·····	492
4. 政策·····	493
5. 部长的角色与责任·····	493
6. 对口联邦机构的角色与责任·····	494
7. 其他部、局和办公室的角色与责任·····	494
8. 与私营部门协调·····	495
9. 国家特殊安全事件·····	495
10. 实施·····	496
<b>二十、第 54 号国家安全总统令：国家网络安全综合计划（节选）·····</b>	<b>498</b>
译者注·····	499
1. 可信互联网连接·····	499
2. 爱因斯坦 2 项目·····	499
3. 爱因斯坦 3 项目·····	500
4. 研发·····	500
5. 态势感知·····	500
6. 反情报计划·····	501
7. 涉密网安全·····	501

8. 网络安全教育 .....	501
9. 新技术 .....	501
10. 网络威慑 .....	502
11. 供应链安全 .....	502
12. 联邦在关键基础设施安全中的角色 .....	502
<b>二十一、网络空间政策评估：保障可信和坚韧的信息和通信基础设施 .....</b>	<b>503</b>
序 .....	504
执行摘要 .....	504
引言 .....	507
1. 从顶层加强领导 .....	510
2. 打造数字化国家能力 .....	514
3. 共同承担网络安全责任 .....	516
4. 建立有效的信息共享和事件响应框架 .....	519
5. 鼓励创新 .....	523
6. 行动计划 .....	527
<b>二十二、网络空间国际战略 .....</b>	<b>529</b>
序 .....	530
1. 制定网络空间政策 .....	530
2. 网络空间的未来 .....	533
3. 政策优先 .....	539
4. 展望未来 .....	544
<b>二十三、第 21 号总统政策令：关键基础设施安全和韧性 .....</b>	<b>545</b>
1. 介绍 .....	546
2. 政策 .....	546
3. 角色和职责 .....	547
4. 三个战略要求 .....	549
5. 创新和研发 .....	550
6. 指令的实施 .....	550
7. 指定的关键基础设施部门和对口机构 .....	552
8. 定义 .....	553
<b>二十四、第 13636 号行政令：增强关键基础设施网络安全 .....</b>	<b>554</b>
1. 政策 .....	555
2. 关键基础设施 .....	555
3. 政策协调 .....	555
4. 网络安全信息共享 .....	555
5. 隐私和公民自由保护 .....	556
6. 咨询过程 .....	556

7. 减少关键基础设施网络风险的基本框架 .....	556
8. 自愿性关键基础设施网络安全项目 .....	557
9. 标识处于最大风险的关键基础设施 .....	558
10. 框架的采用 .....	558
11. 定义 .....	559
12. 总则 .....	559
<b>二十五、增强关键基础设施网络安全框架（CSF） .....</b>	<b>560</b>
执行摘要 .....	561
1. 框架介绍 .....	562
2. 框架基本要素 .....	564
3. 如何使用本框架 .....	567
<b>二十六、网络威慑政策报告 .....</b>	<b>571</b>
1. 前言 .....	572
2. 美国将试图威慑什么 .....	572
3. 网络威慑战略 .....	573
4. 美国网络威慑政策的组成要素 .....	574
5. 结论 .....	583
<b>二十七、国防部网络战略 .....</b>	<b>584</b>
1. 引言 .....	586
2. 战略内容 .....	590
3. 战略目标 .....	592
4. 实现目标 .....	593
5. 管理战略 .....	600
6. 总结 .....	601
<b>二十八、2015 年网络安全法 .....</b>	<b>602</b>
第 I 章 网络安全信息共享（第 101~111 条） .....	604
第 II 章 国家网络安全增强（第 201~229 条） .....	619
第 III 章 联邦网络安全人员评价（第 301~305 条） .....	633
第 IV 章 其他网络事项（第 401~407 条） .....	635
<b>二十九、国家网络安全行动计划 .....</b>	<b>642</b>
1. 挑战 .....	643
2. 我们的路线 .....	643
3. 国家网络安全促进委员会 .....	644
4. 提升全国网络安全水平 .....	644
5. 威慑、劝阻和终止网络空间恶意活动 .....	647
6. 改进网络空间事件响应 .....	647

7. 保护个人隐私 .....	648
8. 网络安全投入 .....	648
<b>三十、第 41 号总统政策令：美国网络事件协调 .....</b>	<b>649</b>
1. 范围 .....	650
2. 定义 .....	650
3. 事件响应的指导原则 .....	650
4. 并行工作方向 .....	651
5. 针对重大网络事件的联邦政府响应协调框架 .....	652
6. 一致的公共联络 .....	653
7. 与现有政策的关系 .....	653
附录 重大网络事件联邦政府协调框架 .....	653
<b>三十一、国家网络事件响应计划 .....</b>	<b>658</b>
1. 执行摘要 .....	659
2. 简介 .....	660
3. 范围 .....	661
4. 与国家战备体系的关系 .....	662
5. 角色和责任 .....	663
6. 核心功能 .....	672
7. 协调结构和整合 .....	674
8. 结论 .....	682
附录 A 政策法规 .....	682
附录 B 网络事件严重度图示 .....	683
附录 C 网络事件严重度图示和国家响应协调中心激活等级的对照 .....	684
附录 D 向联邦政府报告网络事件 .....	685
附录 E 联邦网络安全中心的角色 .....	687
附录 F 核心功能和关键任务 .....	688
附录 G 制定内部网络事件响应计划 .....	692
附录 H 核心功能、NIST 网络安全框架和 PPD-41 的对照 .....	695
附录 I 其他资源 .....	697
<b>三十二、“国家网络安全促进委员会”报告（节选） .....</b>	<b>698</b>
摘要 .....	699
附录 A 要求、建议和行动措施 .....	701
<b>三十三、强化美国网络安全和能力行政令草案 .....</b>	<b>705</b>
1. 政策 .....	706
2. 发现 .....	706
3. 定义 .....	706
4. 政策协调 .....	707



5. 网络脆弱性评估.....	707
6. 对网络对手的评估.....	707
7. 美国网络能力评估.....	708
8. 私营部门基础设施激励报告 .....	708
9. 一般条款 .....	708
<b>三十四、强化联邦网络和关键基础设施网络安全行政令草案.....</b>	<b>710</b>
1. 联邦网络安全.....	711
2. 关键基础设施网络安全.....	712
3. 国家网络安全.....	713
4. 一般条款 .....	714
<b>三十五、强化联邦网络和关键基础设施网络安全行政令 .....</b>	<b>715</b>
1. 联邦网络安全.....	716
2. 关键基础设施网络安全 .....	718
3. 国家网络安全.....	719
4. 定义 .....	720
5. 一般条款 .....	720
<b>三十六、保护网络资产：应对关键基础设施面临的紧迫网络威胁（草稿） .....</b>	<b>721</b>
1. 执行摘要——要点导读 .....	722
2. 介绍 .....	723
3. 建议和依据 .....	724
4. 目标：根本性改变.....	732
附录 A 研究方法 .....	732
附录 B 致谢.....	734
附录 C 关键部门面临网络威胁的紧迫性 .....	734
附录 D 国家网络治理：英国和以色列模式 .....	738
附录 E 参考文献 .....	740
<b>附录 I 美国 CSIS 对特朗普政府的网络安全建议（摘要） .....</b>	<b>755</b>
1. 政策 .....	756
2. 组织 .....	759
3. 资源 .....	759
<b>附录 II 主要缩略语.....</b>	<b>761</b>
<b>致谢 .....</b>	<b>773</b>



---

# 一、第 63 号总统决定令：克林顿政府对关键基础设施保护的政策

1998 年 5 月 22 日

---

本白皮书解释了克林顿政府对关键基础设施保护的政策。我们希望它能够在私营部门和公共部门所有感兴趣的团体中得到传播。我们还希望它能够应用于美国政府专业教育机构，如国防大学和国家外事培训中心，使它们在跨机构的操作及规程上得到课程学习和锻炼。美国政府的所有机构都支持这一非涉密性质的白皮书广为传播。

## 1. 日益增长的潜在脆弱性

美国同时拥有世界最强大的军队以及最强盛的国家经济，我们国力的这两个方面互为补充并互相依赖。而且，它们越来越依靠某些关键基础设施以及基于计算机和网络的信息系统。

关键基础设施是那些物理系统和以计算机和网络为基础的系统，它们对于最基本的经济运行和政府运转非常关键。这些关键基础设施包括但不限于政府和私营部门拥有的电信、能源、银行与金融、运输、供水系统和应急服务。在历史上，国家的很多关键基础设施都是物理和逻辑上分离的系统，彼此之间依赖性不强。然而，随着信息技术的发展以及对提高效率的要求，这些基础设施逐渐变得自动化和互联。这种进步产生了一些新的脆弱性，这些脆弱性将导致设备故障、人为错误、天气和其他自然灾害以及物理和信息攻击。解决这些脆弱性离不开灵活、渐进的方法，以横跨公共和私营部门，对国内和国际安全提供保护。

由于我们的军事力量（强大），未来的敌人——国家、集团或者个人将有可能通过非常规的手段对我们造成伤害，包括在美国本土发动攻击。我们的经济越来越依靠那些互依赖的、由计算机和网络支持的基础设施，对我们的基础设施和信息系统的非常规攻击有可能使我们的军事和经济力量遭到巨大伤害。

## 2. 总统的意愿

长久以来，保障关键基础设施的连续性和生存力一直是美国政府的政策。我希望，美国政府要采取所有必要的措施来迅速减弱我们的关键基础设施，尤其包括我们的信息系统在面临物理和信息攻击时的任何重大脆弱性。

## 3. 国家目标

最迟不晚于 2000 年，美国应当实现初步的信息保障能力；从这份总统令发布之日起，五年后美国将已经获得并保持对我国的关键基础设施进行保护的能力，以防止可能会严重危害到下述职能的有预谋的行为：

- 联邦政府履行其重要的国家安全责任并确保公众健康和安全。
- 州和地方政府维持有序运转，提供最起码的重要公共服务。
- 私营部门确保经济有序运行以及重要电信、能源、金融和运输服务的正常提供。

这些关键功能遭到的任何破坏或操纵必须控制在历时短、频率小、可控、地域上可隔离以及对美国的利益损害最小的规模上。

## 4. 公共-私营合作联盟以减少脆弱性

对我们的关键基础设施的攻击目标将很可能包括经济以及政府部门中的设施，因此需要密切协调公共和私营部门的工作来消除潜在的脆弱性。为取得成功，这一合作联盟必须是真正的、相互的和协作的。为了达到我们的国家目标，消除我们关键基础设施中的脆弱性，美国政府应该在最大可能的程度上努力避免造成政府法规的增多，尽量避免对私营部门发放没有资金支持的政府训令。

对于我们经济中的每个易于受到基础设施攻击的大型部门来说，联邦政府将从指定的领导机构中指派一名高级官员，作为部门联络官来与私营部门合作。经过与他们所负责的基础设施领域内的私营部门实体的交流和合作，部门联络官将确定一个私营部门内代表该部门的合作者（部门协调员）。

部门联络官、部门协调员以及他们所代表的政府机构和公司应该完成下列工作，以促成各自部门级“国家基础设施保障计划”的制定：

- 评估该部门对计算机或物理攻击的脆弱性。
- 推荐用以消除重大脆弱性的计划。
- 提出用来标识并预防大规模攻击的系统。
- 制定下列行动计划：在受到攻击的过程中对该攻击进行报警，控制并切断攻击，随后，在攻击的余波之中，必要时与 FEMA（联邦应急管理局）协商，迅速重建最基本的重要职能。

在每篇部门级计划的准备过程中，国家协调员（见 VI）应该与领导机构的部门联络官、国家经济委员会的代表一起确保各计划的全面协调及整合，尤其要注意其中的相互依赖性。

## 5. 方针

为了消除这些潜在的脆弱性，并阐明消除这些脆弱性的手段，我希望有关人员能够在头脑中牢记如下的普遍原则和事项：

- 针对那些旨在满足总统令目标的方法和项目，我们必须向国会咨询，并努力寻求国会的参与。
- 对我们的关键基础设施的保护必须是一种在关键基础设施所有者、运营者和政府之间共同承担的责任以及一种合作性质的关系。
- 应该时常评估我们的关键基础设施的现有依赖性、脆弱性和威胁环境，因为我们的关键基础设施所面临的威胁的性质一直在迅速地变化着，因此我们的保护措施和响应必须具有充分的适应性。
- 市场诱因是解决关键基础设施保护问题的首选，只有在市场无法为保护美国人民的健康、劳动安全和福利而提供足够资源的时候，才可以诉诸法规。此时，各机构应该确定并评估可行的替代方案，以指导法规的执行，包括提供经济刺激以促进预期行为的实现，或对私营部门的备选方案提供有关信息。这些刺激以及其他的有关行

动应当有助于与最新的技术保持协调，应当引入对国际问题的全局性解决方案，应当使私营部门的所有者和运营者可以获取并维持最大可能的安全性。

- 政府的各级机构、政府的所有功能以及资源，包括执法、法规条例、国外情报和国防战备等功能应在必要的时候使用，以确保关键基础设施得到保护，并维持这种保护状态。
- 必须对私有财产给予认真的尊重。必须使消费者和运营者有这样的信心：他们的信息得到了正确、安全和可靠的处理。
- 通过研究、开发和采购，联邦政府应当鼓励对有效的基础设施保护方法进行引进。
- 在如何最佳地实现基础设施保障这一问题上，联邦政府应当成为私营部门的楷模，并且，联邦政府应当使其工作的成果在最大范围内得到传播。
- 我们必须关注预防性措施以及威胁和风险管理。为此，应当鼓励私营部门的所有者和运营者为他们所控制的基础设施提供最大可能的安全性，并鼓励他们向政府提供必要的信息，以利于政府协助他们实现这个目标。为了使私营部门能全面投入，私营部门所有者和运营者对于是否参与国家基础设施保护系统是自愿的。
- 对于一个稳健、灵活的基础设施保护项目来说，同州政府、地方政府以及第一时间响应人员的密切合作与协调是非常重要的。所有的关键基础设施保护计划和行动应当将州、地方政府和第一时间响应人员的需求、活动和责任考虑进去。

## 6. 结构和组织

为了达到我们的目标，联邦政府应当围绕四个部分进行组织（附录 A 详述）。

（1）作为部门联络的领导机构：对每个有可能成为信息或物理攻击目标的基础设施部门来说，将唯一的联邦部局作为联络时的领导机构。每个领导机构将指派一名相当于助理部长或更高级别的人来担任该基础设施领域内的部门联络官，他应与私营部门的代表（部门协调员）一起解决与关键基础设施保护有关的问题，尤其是一起为国家基础设施保障计划添砖加瓦。领导机构和相对应的私营部门将制定并执行该部门的脆弱性意识和教育项目。

（2）特殊职能的领导机构：除上述之外，某些关键基础设施保护职能必须主要由联邦政府执行（国防、外事、情报、执法），对其中的每项特殊职能，都应有一个领导机构负责协调美国政府在该领域内的活动。每个领导机构将指派一名助理部长和更高级别的高级官员来担任联邦政府的职能协调员。

（3）跨机构协调：领导机构的部门联络官、功能协调员以及来自其他相关机构和部局，包括国家经济委员会的代表，需要在关键基础设施协调组（CICG）的帮助下，一起协调本总统令的执行。CICG 由安全、基础设施保护和反恐怖主义国家协调员领导。国家协调员将由总统指派并通过总统国家安全事务助理向总统汇报，国家安全事务助理则应当确保与总统经济事务助理的协调。CICG 内各机构的代表应当具有较高级别（助理部长和更高）。在必要的时候，CICG 将得到外部政策组织的协助，比如安全政策委员会、安全政策论坛、国家安全和电信委员会以及信息系统安全委员会。

（4）国家基础设施保障委员会：由领导机构、国家经济委员会和国家协调员推荐，总统将指派一个由大型基础设施提供商和州及地方官员组成的小组组成国家基础设施保障委员

会，委员会主席由总统指定。国家协调员将担任该委员会的执行主任。国家基础设施保障委员会将定期集会，以加强关键基础设施保护中公共和私营部门间的合作关系，并在必要的时候向总统提交报告。联邦政府的高级官员也可以适时参加国家基础设施保障委员会的会议。

## 7. 保护联邦政府的关键基础设施

联邦政府的任何一个部局都应该负起保护其自身关键基础设施的责任，尤其是保护其基于计算机和网络的系统。任何部局的首席信息官（CIO）应对信息保障负责。任何一个部局都应当指派一名首席基础设施保障官（CIAO），他应对该部门的关键基础设施的其他所有方面的保护工作负责。首席信息官和首席信息保障官也可以是同一个人，具体由每个机构自己决定。这些官员应当建立起获取有效授权的步骤，以获准对政府的计算机和信息系统执行脆弱性评估。司法部将为这种授权制定法律方针。

从这部总统令的发布时起，不超过 180 天，每个部局都应该制定其保护自身关键基础设施的计划，包括但不限于基于计算机和网络的系统。国家协调员将负责协调各部局对跨机构依赖性所做的分析并协调对这种依赖性的消除行动。关键基础设施协调组（CICG）将发起一个对这些计划的专家评审过程。从现在起，不迟于两年，这些计划应得到执行，并在以后每两年更新一次。为满足这一时间进度，在如何最佳地保护关键基础设施这一问题上，联邦政府应当成为私营部门所参照的楷模。

## 8. 任务

在 180 天内，首脑委员会应当向总统提交一份制定国家基础设施保障计划的日程表，其中要有完成下述相关任务的时间表。

（1）脆弱性分析：对每个有可能成为严重的基础设施攻击目标的经济部门和政府部门来说，首先应该发起脆弱性评估，并定期更新这种脆弱性评估活动。必要时，这些评估活动还应该包括在每一部门中确定极为重要的基础设施的最小集。

（2）矫正计划：基于脆弱性评估，还应该推荐一个矫正计划。在计划中应当确定脆弱性矫正的时间期限、责任和基金。

（3）预警：应当立即建立一个对重大基础设施攻击发出预警的国家中心（见附录 A）。我们将尽快部署一个增强系统，用于检测和分析这类攻击，并且希望得到私营部门最大可能的参与。

（4）响应：应当建立起在系统运行时对重大基础设施攻击进行响应的系统，目标是对破坏进行隔离并使其影响减至最小。

（5）重建：在面对业已成功各种规模的基础设施攻击时，我们的重建系统都能够立刻重新建立起最基本的期望功能。

（6）教育和意识培养：在政府和私营部门内，都应该有针对脆弱性的意识培养和教育项目，以使人们对于安全的重要性有感性认识并在安全标准，尤其是信息系统的安全标准方面对他们进行培训。

(7) 研究和开发：应该对由政府发起的基础设施保护研发活动进行协调，应该制定多年度的研发计划，将私营部门的研究考虑进去，并且要得到充足的资金支持，从而在一个短暂但可行的时间段内使脆弱性减至最小。

(8) 情报：情报共同体应当制定并执行一个相关计划，以加强收集和分析我国的基础设施面临的国外威胁，包括但不限于国外的计算机/信息战威胁。

(9) 国际合作：应当有一个相关计划，在关键基础设施保护方面，拓宽与意识形态相似的国家、友好国家、国际组织和跨国公司的合作。

(10) 立法和预算要求：应当评估行政部门中涉及关键基础设施的法律依据以及预算优先权，在必要时向总统提交修订建议。任何评估和建议都应当与预算和管理办公室（OMB）主任保持协调。

CICG 还应该评审附录 B 中所列的任务并对其做出安排。

9. 执行

除了前面提到的要在 180 天之内提交的报告外，国家协调员还应该在与国家经济委员会的合作下，通过总统国家安全事务助理向总统和各部局的领导提交一份有关本总统令的执行情况的年度报告。报告中应当包括更新后的脆弱性评估、对国家计划和其他政策中确定的任务段的完成情况、立法和预算方面的建议。任何评估和建议都应当与预算和管理办公室（OMB）主任保持协调。此外，当 2000 年我们建立初步的信息保障能力后，国家协调员应当对其重新进行评估。

附录 A 结构和组织

领导机构

必须在美国政府内为特定的部门和职能制定清晰的责任。责任分配如下。  
作为部门联络的领导机构：

商务部	信息与通信
财政部	银行与金融
环境保护局（EPA）	供水
交通部	航空、高速公路（包括汽运和智能运输系统）、大宗货物运输、输运管道、铁路、水路贸易
司法部/FBI	应急执法服务
联邦应急管理局（FEMA）	应急消防服务，政府服务连续性
健康和公众服务部（HHS）	公共健康服务，包括预防、监测、实验室服务以及公民健康服务
能源部	电力、石油和天然气生产和储存



针对特殊职能的领导机构：

司法部/FBI	执法和国内安全
中央情报局	外国情报
国务院	国外事务
国防部	国防事务

此外，通过国家科技委员会，科技政策办公室（OSTP）将负责研发日程和研发项目的协调。而且，虽然商务部是信息与通信的领导机构，但国防部仍将保留其对国家通信系统的执行责任并负责对总统的国家安全电信咨询委员会提供支持。

### 国家协调员

安全、基础设施保护和反恐怖主义国家协调员应当负责协调本总统令的执行。国家协调员将通过总统国家安全事务助理向总统汇报。当部长级会议和首脑委员会讨论基础设施问题时，国家协调员将作为正式成员参加。虽然国家协调员不能直接指挥政府各部局，但他将确保政策制定和执行时的跨机构协调，并将评审那些涉及国外因素的基础设施事件的危机处理行动。在制定年度预算时，国家协调员将提供有关关键基础设施保护的机构预算建议。国家协调员还将主持关键基础设施协调组（CICG），向部长级会议做出报告（或应首脑委员会主席的要求做出报告）。部门联络官和特殊职能协调员将参加 CICG 的会议。各部局应当各指派一名高级官员（助理部长级或更高）定期出席 CICG 会议。国家安全顾问应当在国家安全委员会成员中指派一名基础设施保护资深主任。

国家计划协调处（NPC）的成员由各个部门无条件提供。NPC 将把各个部门的计划整合进国家基础设施保障计划之中，并协调美国政府对关键基础设施依赖性的分析。NPC 还将协调国家的教育和意识培养项目以及法律和公共事务。

国防部应当继续担当人事调动办公室的行政机关，在 1998 年剩下的时间中，人事调动办公室将是构成 NPC 的基础。从 1999 年开始，NPC 将成为商务部的一个办公室。人事管理办公室（OPM）将为促进 NPC 的运转而提供必要的协助。在 2001 年底，NPC 将消亡，除非总统令将其延期。

### 预警和信息中心

作为国家预警和信息共享系统的一部分，总统很快授权联邦调查局（FBI）将其现有的组织结构扩展成一个大规模的国家基础设施保护中心（NIPC），该组织将作为国家的关键基础设施威胁评估、报警、脆弱性和执法调查、响应实体。在最初的 6~12 个月内，总统还指示，国家协调员和部门联络官要与部门协调员、特殊职能协调员、来自国家经济委员会的代表在必要的时候一起合作，向关键基础设施的所有者和运营者咨询，鼓励他们建立私营部门的共享和分析中心，如下描述。

（1）国家基础设施保护中心（NIPC）：NIPC 将包括 FBI、USSS 以及其他在计算机犯罪和基础设施保护领域富有经验的调查员，还包括来自国防部、情报共同体以及领导机构的一些代表。NIPC 将以电子的方式连到联邦政府的其余部局中，包括其他的预警和运营中心以及任何私营部门的共享和分析中心。它的任务将包括对国际威胁提供实时的报警、综合的分析以及执法调查和响应活动。

所有的行政部局都应 与 NIPC 合作，在法律许可的范围内应其要求提供支持以及信息和建议。在法律许可的范围内，所有的行政部局还应共享 NIPC 的威胁信息、攻击预警以及针对政府和私营部门关键基础设施的实际攻击的信息。NIPC 将包括负责下列事务的组成单位：预警，分析，计算机调查，应急响应的协调、培训、推广，以及技术工具开发和应用。此外，它还将直接同私营部门中的一些机构以及由私营部门创建的信息共享和分析实体，比如下面将谈到的信息共享和分析中心，建立联系。

在与信息源提供机构的合作下，NIPC 将对执法机关和情报组织提供的信息进行过滤，以便将这些信息纳入分析和报告之中。这些分析和报告将以合适的格式提供给相关的联邦、州和地方政府的机构，相关的关键基础设施所有者和运营者，任何私营部门的信息共享和分析中心实体。当传播来自于国家安全信息或情报共同体的其他信息时，NIPC 将通过现有的流程与情报共同体保持全面协调。不论报告是否经过过滤，NIPC 都将据此发布攻击预警，使私营部门的信息共享和分析中心实体以及关键基础设施所有者和运营者进入威胁来临状态。这些警报中还包括对基础设施所有者和运营者可以采取的补充保护措施的指导。在极端紧急的情况下，NIPC 在对即将到来的国际恐怖主义袭击、国外政府攻击或其他国外邪恶力量攻击发布全面预警之前，将同国家协调员进行协调。

NIPC 将成为收集基础设施威胁信息的国家级中心机构，除此之外，NIPC 还将提供一些重要的途径来加速并协调联邦政府对事件的响应、对攻击的防御、对威胁的调查以及对重建工作的监控。根据国外威胁/攻击的性质、在特殊职能机构（司法部、国防部、中央情报局等）间达成的协议以及总统的最终决定，NIPC 可能会直接向国防部或情报共同体提供支持。

（2）信息共享和分析中心（ISAC）：在与部门协调员、部门联络官和国家经济委员会的合作下，国家协调员将向关键基础设施的所有者和运营者咨询，强烈鼓励他们创建私营部门的信息共享和分析中心。通过与联邦政府的商议和政府的协助，中心的实际设计、功能及其同 NIPC 的关系将由私营部门自己决定。在本总统令发布的 180 天内，经过 CIGC（以及国家经济委员会）的协助，国家协调员将确定联邦政府用以对 ISAC 提供援助的可能方法，以促进 ISAC 的启动。

ISAC 将成为收集、分析、适当过滤私营部门的信息并向工业界和 NIPC 传播信息的一种机制，还将收集、分析和传播来自于 NIPC 的信息，以使这些信息进一步向私营部门发布。对于成熟的政府-工业界合作联盟来说，该机制虽然很原始，但是这种对脆弱性、威胁、入侵和异常现象进行重要信息共享的机制并不会对公司和政府间的直接信息交换造成干扰。

根据私营部门代表的最终设计，ISAC 将参考灾难控制和防御中心等机构的某些特色，后者已经被证明非常有效，尤其是在同私营部门和非联邦部门的大量信息的互换方面。在这样的模式下，ISAC 将拥有非常广泛的技术主题和专业技术以及大量非法令性的、非执法机构性的任务。它将建立起各类基础设施的基本统计数据 and 模式，成为机构内部以及各类机构之间的数据交换所，提供可供私营部门使用的历史数据图书馆，在 ISAC 认为合适的情况下，这个历史数据图书馆可供政府使用。对 ISAC 的成功异常重要的是及时性、可访问性、协调性、灵活性、实用性以及可接受性。

## 附录 B 其他任务

### 研究

国家协调员应当对下列专题展开委托研究：

- 由于私营部门公司参与信息共享过程而引发的责任问题。
- 信息共享所面临的法律障碍以及对消除这些障碍的提议的审查，包括通过与美国法律学会的协调来起草标准法令。
- 文档化和信息分级的必要性，这种分级对信息传播带来的影响，以及既可以用来安全地共享威胁和脆弱性信息，又可避免信息泄露或被滥用者获取的信息共享方法和系统。
- 增强对下列信息的保护（包括这些信息的安全传播系统和处理系统）：工业贸易秘密以及其他的保密性商业数据、执法机关的信息和证据、保密的国家安全信息、有可能泄露私营基础设施脆弱性的非涉密材料以及其他虽然无害但也不适宜泄露的某些信息。
- 当有必要为了美国的基础设施的安全而与国外实体共享信息时，这种信息共享带来的影响。
- 对关键基础设施提供商的保险条例进行命令、资助或协助时，这方面的安全标准的潜在裨益；对于希望同美国进行贸易的国外关键基础设施提供商，要求其保险相关联的有关安全标准的潜在裨益。

### 公共推广

为了增强公众对基础设施保护的感性认识，应当采取下列行动：

- 在国家协调员的关注下，白宫应当同有关的内阁机构一起考虑召开一系列会议：
  - ①使公共和私营部门中的国家领导走到一起，提出旨在增强信息安全职责的有关项目；
  - ②召集来自工程界、计算机科学、商学院和法学院的学术领袖，评审信息安全教育现状，确定需要对课程和资源做出哪些必要的改变，以满足国家对信息安全领域内的专家需求；
  - ③讨论与 K~12 年级以及普通大学的学生有关的计算机伦理学问题。
- 国家科学院和国家工程院应考虑召开圆桌会议，把联邦、州和地方政府的官员们以及工业界和学术界的领袖们召集到一起，制定用以增强基础设施安全的国家战略。
- 情报共同体以及执法机关应当对现有的项目做出扩展，以利于向基础设施所有者、运营者以及高级政府官员做出简单通报。
- 国家协调员将①建立一个模拟基础设施保障的项目，该项目要涉及公共和私营部门的高级官员，对该项目的报告将作为意识培养运动的一部分来公布；②在与私营部门的协调下，发起一个连续性的意识培养国家项目，强调增强基础设施安全性的重要性。

### 联邦政府内部的活动

为了使联邦政府能够改善其基础设施安全，下述行动应立即开始执行：

- 商务部、总务管理局（GSA）以及国防部应该协助联邦各机构在其各自的机构内部执行信息保障的最佳实践措施。
- 国家协调员将协调对联邦、州和地方政府中担负信息保障任务的实体所进行的评审，提出推荐性意见，指出这些机构如何才能最有效率地展开合作。
- 所有的联邦机构都应该清楚地指明负责对该机构的计算机系统进行访问授权的人选。
- 要增强对国外信息战威胁信息的收集和分析，情报共同体应当评估该项活动的优先权，并将这种优先权进行形式化。
- 联邦调查局、特工处以及其他的有关单位将①极力招募具有相关计算机技术技能的本科生和研究生，使他们以全职或兼职的形式受雇于地区计算机犯罪行动组；②加大对拥有计算机攻击分析和调查技术的合格人员的雇佣和留任。
- 在向国防部咨询后，交通部应该对依赖于全球定位系统（GPS）的国家运输网络的脆弱性进行彻底评估。这项工作包括对基于 GPS 的民事用户所面临的风险进行一次独立的、综合的评估，同时基于这些评估决定现代化 NAS 的最终体系结构。
- 联邦航空管理局应当制定并执行一个综合性的国家航空系统安全项目，以保护现代化的 NAS 网络，使其免于信息攻击或其他破坏。
- 总务管理局（GSA）应当确定同基础设施保障有关的大型采购任务（比如新的联邦电信系统 FTS2000），研究采购过程是否反映了信息保护的重要性，并且在必要的时候应拿出有关提议，对整体的采购过程进行修改，从而有利于信息保护。
- 管理和预算办公室（OMB）应当指导各联邦机构把所分配的基础设施保障职能列入《政府绩效和结果法》战略计划的制定和政府绩效评估框架之中。
- 根据 NSD-42 中说明的国家职责，国家安全局（NSA）应当对美国政府的系统进行评估，发布威胁和脆弱性信息，建立标准，展开研发，并负责评估安全产品。

### 协助私营部门

为了协助私营部门实现并维护其基础设施的安全，应进行以下活动：

- 国家协调员和国家基础设施保障委员会应拿出提议并制定行动路线来激励私营部门对其关键资产，包括信息和电信系统执行定性的风险评估。
- 商务部和国防部应当合作，通过与私营部门的协调，向私营部门的关键基础设施所有者和运营者提供专业知识，以制定最佳安全实践规范。
- 司法部和财政部应当发起一次综合性的研究工作，编纂计算机犯罪方面的人口统计学资料，比较各州对计算机犯罪的处理方法，制定有关方案来阻止青少年计算机犯罪，并对这些犯罪做出响应。

---

## 二、保护美国的网络空间——信息系统保护国家计划

美国白宫  
2000年1月7日

---

## 总统的话

华盛顿 白宫

在不足一代人的时间内，信息革命和计算机在社会各个层面的引入已经改变了我们的经济运行方式、我们保障国家安全的方式以及我们日常生活的组织方式。不论是仅仅在家中打开电灯的开关、登上飞机，还是当我们的亲人生病了我們寻求帮助，我们都要依赖于一个或者多个复杂的计算机驱动系统。同样，我们最为复杂的国防系统所依赖的很多商业、通信和运输业也都是由计算机控制的。将来，计算机技术将继续为美国人民创造新的机会。

然而，这个充满希望的时代也充斥着危险。所有受计算机驱动的系统都容易遭到入侵和破坏。我们的经济部门或者政府机构的计算机一旦受到合力攻击，就会产生灾难性的后果。

我们知道，这种威胁是事实存在的。曾几何时，我们的对手只是依赖于炸弹和子弹，而如今，一台笔记本电脑就可以成为敌对分子和恐怖分子可能利用的武器，从而给我们带来巨大的破坏。如果我们想继续享用信息时代所带来的种种益处，捍卫我们的安全，保卫我们的经济成果，那么就必须保护我们重要的计算机控制系统免受攻击。

这就是为什么在审阅了总统委员会关于关键基础设施保护的报告后，我在 1998 年 5 月发布第 63 号总统令的主要原因。这个总统令要求行政部门评估国家关键基础设施的计算机脆弱性，这些基础设施包括信息与通信系统、能源部门、银行与金融业、运输业、供水系统、应急服务部门、公共安全以及负责联邦、州和地方政府职能连续性的领导机构。该总统令着重强调了要保护政府自身的关键资产以使其免受计算机攻击，同时还强调了对缺陷进行矫正的需要，目的是使政府成为信息安全的典范。总统令还要求联邦政府制定保卫国家免受计算机破坏的详细计划。

信息系统保护国家计划是一系列更为复杂的工作的第一步。随着我们对正在出现的威胁和脆弱性的认识不断深入，我们的计算机保护计划将持续发展和更新。它向我们展示了一个综合性的方案，为我们的经济、国家安全、公共健康和安全中的关键部门提供了保护措施。

为了使这个计划成功实施，政府和私营业主必须齐心协力，结成一种前所未有的合作关系。只有举国上下团结应战，才能实现我们的目标。因此，我已经要求内阁成员与作为关键基础设施运营者的私营工业和公共服务部门的代表进行密切的合作。我们不能指望政府法令来实现我们的目标，每个部门都必须自己决定保护其关键系统所必需的方法、步骤和标准。作为这种合作联盟中的一方，联邦政府随时准备提供帮助。

当然，联邦政府也有自己的重要任务，这包括在计算机安全领域开展研发，培育青年科学家来帮助保护我们的联邦计算机系统，协助私营部门制定其保护信息技术的措施。

当推进我们的计划时，所有美国人都应该知道，加强我们的计算机保护措施不能也绝不会以公民的自由作为代价。我们绝不能危害我们恰恰要极力保护的自由。

我在计划里建立的各个任务时间表是很宏大的，实现它们需要我们国家领导阶层的持续支持、紧密的公共-私营合作以及必要的法律和财政拨款。然而，这是一个我们现在就必须着手启动的重要任务，这样，我们才能享用信息时代提供的众多机会，并为下世纪的繁荣和发展建立我们所必需的安全基础。

——克林顿

## 国家协调员的话

这个计划是世界上第一次由国家政府实施的、用来设计其国家的网络空间保护方案的尝试活动。

### 美国的新依赖——美国的新威胁

比起其他国家来，美国对其网络空间的依赖性更强。对国家网络空间的攻击可以破坏我们的输电线路、电话网络、运输系统以及金融机构。所有这些部门都依赖于涉及计算机系统的控制网络。

在下一场战争中，敌人的目标将是美国的基础设施，敌人的新武器将是针对我们的关键网络和系统的计算机攻击。我们知道有些政府正在发展这种能力。

因此，我们需要重新设计国家的信息基础设施的结构。在上个十年，我们的信息基础设施建设非常迅速，但没有对安全给予足够的关心，没有考虑到富有经验的敌人会去攻击它。而现在我们则必须对其做出改动，以对其进行保护、防止攻击或减小业已存在的脆弱性。

总统已经要求制定一个网络空间保护计划，且这个计划要在 2000 年 12 月前初步生效，到 2003 年 5 月完全施行。为了达到这个目标，我们必须迅速行动，因为我们有很多事情要做。

### 真正的公共-私营合作——非指令性的解决方案

总统要求联邦政府成为计算机系统安全的典范，但现在事实还并非如此。国防部在建立安全系统方面做得非常好，但同样关键的民事机构却通常没有充分地得到对计算机系统攻击的保护。这个计划提出了国防部和其他联邦政府部门要采取的很多后续步骤。

私营业主的基础设施至少也是计算机系统攻击的目标。在现代社会，关键的工业和公共事业已经成为各种冲突中的破坏目标。美国的国力就在于私营业主所拥有和运营的很多关键基础设施和工业。

私营业主拥有的计算机网络正处在被扫描和渗透之下，某种情况中还成为破坏、偷窃、间谍活动和攻击的目标。虽然总统和国会能够命令联邦网络实现安全化，但他们不能也不应该为私营部门的系统规定解决方案。

因此，在本阶段，这个计划对私营网络的安全和保护不做具体安排，只是为其建议一个公共框架。一些私营机构已经决定联合起来保护它们的计算机网络。当它们进行这些活动时，联邦政府能够而且必将会帮助它们。然而，政府将不会指示解决方案，并且避免做出条例规定。政府也不会侵害公民自由、隐私权或私有信息。

这是国家计划的第一版。为了使它能得到改进，我们真诚地征求大家对这一计划的评论。一旦私营部门实体做出了更进一步的减小脆弱性和加强保护措施的决定和计划，这些进步将会在本计划的后续版本中得到反映。

### 解决方案的各个组成部分——首先是经过培训的人员

正如您将在文中看到的，这个计划将为我们的网络空间建立防御，它依赖的是新的安全标准、多层次的防御技术、新的研究以及对人才的培训。其中最为急需但最难以达到和实现的就是具有一个受过培训的计算机科学家和信息技术（IT）专家核心。

一个世纪以前，为了电力的应用，美国迅速实现了电线布线，国家马上为这个新的经济培训出了电气学家和电气工程师。但迄今为止，面对刚刚出现的以 IT 为基础的新经济，美国还没有培训出能有效负责其运行、改进并保护其安全的 IT 专家。这个计划将提出一系列步骤来刺激高等教育，培养出美国在这一领域所迫切需要的人才。

继我们的计算机防御计划之后，我们将推出第二个计划。后者将集中关注政府怎样与国家的基础设施部门合作来确保那些重要服务的可靠性和安全性，使其免受大规模的破坏。这个即将推出的计划主要依赖于各公司和机构的投入。这些公司和机构中各种各样的复杂网络正为美国人民提供着经济福利、健康、保险及安全。

### 人民和国会

这个计划是联邦政府中很多人士广泛工作的结果。以他们的名义，我们把这个计划提供给全国人民以及各众议员，希望举国努力来改善这一计划，保卫我们的网络空间，保卫依赖于这个网络空间的所有力量和我们人民。

——理查德·克拉克

安全、基础设施保护和反恐恐怖主义国家协调员

### 介绍

在这个世纪之交，联邦政府和私营业主齐心协力，使我们平稳过渡到了 2000 年。为了避免千年虫可能造成的信息系统故障和服务崩溃，我们曾做了广泛的准备，现在这些准备已见成效，关键系统保持了持续运行，没有出现任何重大故障。这些事情说明，必须记住我们处在一个动态的环境中，计算机攻击的性质和我们为保护信息系统所做的准备将始终处在变化之中。随着新的保护措施的发展并投入使用，那些试图攻击我们的人也会变得更加具有创新性。现在联邦政府正在评价千年虫防御的经验，用来决定未来防御计算机攻击的持续措施的各个相关方面。

这个文件是世界上第一次由国家政府实施的、用来设计国家的网络空间保护方案的尝试活动。总统曾在第 63 号总统令中对其制定做了指示。把它指定为“版本 1.0”，表明了这个计划还处于发展的初期，还有很多工作要继续。

当前这部计划的第一个版本主要集中关注联邦政府为保护国家中以计算机为基础的关键基础设施所做的国内工作。后继版本将包含 PDD63 中所考虑的更广泛的内容，包括工业界、州和地方政府在保护私营的基础设施时——单独或与政府合作——所起的作用以及对物理基础设施的保护和关键基础设施的保护中国际事务的思考。为了改善我们的计划，我们广泛征求工业、国会、州和地方政府以及普通公众的评述，在后继版本中，这些评论将被包含进去。

### 什么是关键基础设施系统和资产

关键基础设施是指那些对国家中十分重要的物理性的以及基于计算机的系统和资产，它们一旦受损或遭到破坏，将会对国家安全、国家经济安全和（或）国家公众健康及保健产生破坏性的冲击。

PDD63 要求国家计划为关键基础设施保护的目标、原则和长期计划制定出优先级次序，在初期阶段，国家计划的重心主要是当前联邦政府的计算机安全和 IT 需求。



## 威胁

在美国，对于政府和工业界内的关键网络进行控制的计算机系统——国防设施、高压输电线、银行、政府机构、电信系统以及运输系统，每天都会受到成千上万次的攻击尝试。

这些攻击尝试中有的以失败告终，有的却取得了成功。有的人获得了“系统管理员的地位”，下载了口令，安装了嗅探器以复制交易信息，或者插入了陷门以方便其以后进入。

有的攻击者就像驾车兜风的窃车者，把犯罪当作一件乐事。有的攻击者则是为了从事间谍活动、偷窃、报复性破坏和勒索。还有的攻击者可能是为了收集情报、预先侦察或者创造未来攻击的能力。这些作恶者种类甚多，从青少年到小偷，从有组织的犯罪团体到恐怖分子，还有潜在的军事敌对力量以及情报机构。这些威胁的严重性在最近几年不断增加。

我们还知道一些外国政府正在为对付美国的计算机网络而发展强大的攻击能力。

美国在基础服务上对计算机网络有越来越多的依赖，以至于很容易受攻击。然而，在国家如此紧密地依赖计算机网络的同时却很少注意保护它。水、电、气、通信（语音和数据）、铁路、航空和其他关键设施都在巨大的信息系统网络中直接受到计算机的控制。

在将来的危机中，罪犯团伙、恐怖分子集团、敌对国家会制造经济破坏、混乱和死亡，并通过攻击这些关键性的网络来降低我们的防御响应能力。中央情报局局长 George Tenet 曾证实：“这种威胁是很现实的。”

## 保护隐私和公民自由

基础设施保护的目标要在与公民的全面自由权益保持一致的前提下得到实现。事实上，一些基础设施保护计划增强了网络环境中数据和通信的安全级别，从而能对个人隐私和其他的公民自由权产生积极的影响。

联邦政府有义务保护其计算机用户的个人信息。政府之所以成为这些信息的信托对象，是因为美国公民相信他们的关键性个人信息能在这些系统中得到安全的保存。

联邦政府意识到，用以保护信息和系统的技术如果使用不当，将会在无意中损害公民的自由。甚至即使初衷是好的，但如果保护入侵的技术使用得太广泛，也可能会波及一些正当的行动。尤其在那些个人权利很敏感或有争议的地方，我们有必要认真地考虑与此相关的一切问题。

在权限、安全标准和认可协定等方面，法律并不总能提供清楚的指导方针。计算机入侵事件经常给我们提出复杂的法律和司法问题。因此，政府保护基础设施和公民自由权利的诸多项目都需要仔细地计划、分析，并要求所有受影响的实体参与。

这篇国家计划中所有的提议都完全符合现行的法律以及人们对隐私保护的期望，同时，计划的某些部分可能促使大家更加关注个人隐私被损害以换取基础设施保障这一问题。

既要使基础设施得到保护，也要与公民的自由权利相一致，寻找这样的解决方案是个动态的过程，必须包括政府和私营业主团体的参与。在这个过程中，必须意识到现有司法制度的复杂性和重要性，还要建立新的项目以防止意外后果的出现。

在这样的大势之下，有几个重要的原则可以作为国家计划中分析其项目的出发点：与隐私权团体协商以定义可行的解决方案；对计划各项目进行严格而彻底的法律评审；遵循已有

的法令和规则；政府必须做出榜样；评审各种各样的隐私解决方案；和国会合作；和国家科学院合作；致力于教育和意识培训；遵循由信息基础设施任务组内的隐私工作组制定的隐私原则。

这篇国家计划是有关如何对联邦计算机安全 和信息资源管理（IRM）责任进行补充的	
国家计划的实施	IRM/管理责任
标识联邦政府内的主要节点和各关键基础设施系统依赖性	OMB：应 OMB A-130 通告附录III“联邦自动化信息资源的安全”的要求，使用这些信息来管理各机构的脆弱性并进行风险评估
标识主要的国家安全资产和基础设施系统	OMB：应 PDD63 的要求，使用这些信息将基础设施保护工作纳入《政府绩效和结果法》（GPRA）的机构报告中
标识基础设施系统需求、依赖性以及共有的威胁和脆弱性	各机构的 CIO/CFO：使用这些信息做出关键基础设施系统预算提议
标识基础设施系统威胁、脆弱性；标识联邦机构中哪些地方存在共有的威胁和脆弱性	各联邦机构：应 A-130 要求，使用这些信息评估各机构中关键性信息系统的脆弱性和风险 OSTP 和 OMB：使用这些信息来制定研究和开发进度
标识并寻求与私营部门伙伴的合作；标识基础设施依赖性 以及共有的威胁和脆弱性	CIO 委员会：使用这些信息来制定私营部门推广计划；充分利用在这篇国家计划的结构下建立的各类关系

### 联邦计算机安全和 IRM（信息资源管理）责任

管理和预算办公室（OMB）承担了联邦计算机安全和信息化管理的核心责任，与我们的国家计划关注国家安全系统并强调与私营企业合作所不同的是，OMB 对联邦自动化信息系统安全政策的制定有着法定的责任。它制定的主要政策包括：

焦 点	法 令
计算机安全和隐私：确保公众对数据的访问	1987 年，计算机安全法
绩效表现和结果：管理各机构的职能表现	1993 年，政府绩效和结果法
效率：最大限度地利用收集到的信息，尽量减小公众对数据请求的负担	1995 年，削减文书工作法
机构管理 IT 的责任：采购、投资、安全，在每一机构中建立 CIO 职位	1996 年，Clinger-Cohen 法
OMB 通过 CIO 委员会的建议和监督来实施其核心原则	行政令 13011

OMB 实现这些要求时主要依靠 OMB A-130 通告的附录III“联邦自动化信息资源的安全”。通告中要求 OMB 监督操作规范和标准的开发以及对脆弱性和风险的评估，还要负责管理公众对信息的访问。OMB A-130 对上述每一事项都有详尽的说明。在过去的几年中，OMB 还发布了很多其他相关资料，涉及如下内容：

- Internet 和网站隐私声明；
- 推荐的计算机操作规范和标准；
- 大型系统的采购。

## 计划概览

这个计划的目标是在 2000 年 12 月之前使关键信息系统的防御性能初步运行，在 2003 年 5 月完全运转。这个系统防御投入运行后，美国将有能力确保：

“这些关键功能遭到的任何破坏或操纵必须控制在历时短、频率小、可控、地域上可隔离以及对美国的利益损害最小这样一个规模上。”——克林顿总统在 PDD63 中所述。

为了达到克林顿总统所确立的在 2003 年建立起对国家关键基础设施的完全防御这一最终目标，这个计划的现行版本围绕三个目标进行设计。

- 准备和防范：减小对我们的关键信息网络进行成功攻击的可能性，建立一个面对类似攻击仍能保持有效运转的基础设施。
- 检测和响应：实时地确定和评估攻击，对攻击进行控制，受攻击后迅速恢复和重建。
- 建立牢固的根基：我们应该为国家培养相关人员，建立相关组织，完善法律和传统，使我们能更好地针对关键信息网络遭到的攻击进行准备、防范以及检测和响应。

为此，计划的 1.0 版本提出了以下 10 项内容。

### （1）准备和防范

- 内容 1：标识关键基础设施资产以及共有的互依赖性，查找其脆弱性。

### （2）检测和响应

- 内容 2：检测攻击和非法入侵。
- 内容 3：开发稳健的情报和执法功能，保持与法律的一致。
- 内容 4：以实时的方式共享攻击预警和信息。
- 内容 5：建立响应、重建和恢复能力。

### （3）建立牢固的根基

- 内容 6：为支持内容 1~5，加强研究和开发。
- 内容 7：培训和雇用足够数量的信息安全专家。
- 内容 8：加强推广，使美国人民知晓加强信息安全的必要性。
- 内容 9：通过立法和拨款，支持内容 1~8。
- 内容 10：在计划的每一步骤和每一部分中，都要确保美国公民的自由权、隐私权以及私有数据保护权得到全面保障。

本摘要将继续描述每项内容及其相应的时间进度。

这篇计划经过了总统的批准，将为联邦各部局准备各自的预算提供全面的方针和指导，但它不是一个用来决定预算的文件。各机构保护其信息系统时的资金拨款决策将依照常规的 OMB（管理和预算办公室）预算步骤做出。

内容 1：标识关键基础设施资产以及共有的互依赖性，查找其脆弱性

“首先，了解你自己。”

第一项内容要求政府和私营部门标识其关键信息网络的重要资产、互依赖性和脆弱性，然后制定并实施实际可行的方案去修复其脆弱性，同时，不断地展开新一轮的评估和修复工作。

对关键信息系统和计算机网络防御做准备的第一个必要步骤就是全面评估关键基础设施系统的资产、互依赖性和脆弱性。我们将不断估计对手对我们的关键基础设施进行破坏的能力。但同时，我们的保护工作必须建立在标识关键基础设施并评估其脆弱性的基础之上。

我们还没有意识到共有的基础设施系统的互依赖性。经验显示，大多数（即使不是全部）信息系统很容易遭受入侵，特别是有内部人员帮助时。虽然有了防火墙和口令系统的广泛应用，但非法入侵还是经常发生。一些防火墙功能有限或者没有经常升级，而且有的技术还可以绕过防火墙。用户经常使用太过简单的口令，或者很少定期更换它们。一些可以通过公开渠道获得的软件程序就能破解口令。用户还有可能在无意中使用了黑客故意给他们的软件，这些软件在整个系统中秘密安装了陷门。还有一些使用者可能违规安装了未授权的调制解调器，这样他们就可以在家里工作，结果在无意中为他人进入网络打开了方便之门。

标识计算机网络资产和脆弱性的主要工作内容是：

- 基于机构/部门之间国家安全和日常任务的区别，确认最关键的资产。
- 分析政府内部或者政府和（或）私营部门之间的共享互操作性。
- 基于对关键资产的确认和共享互操作性的分析，系统管理员、操作者、安全专家和CIO对网络脆弱性进行评估。
- 由受过相关培训的外部专家对这些工作进行评价。

信息系统安全操作规范和标准能够帮助各机构标识并发现脆弱性。虽然很多工作都已经做过，但一个公众可接受的信息系统安全操作规范和标准框架仍处在形成阶段。联邦政府、私营部门和标准制定团体的紧密合作可以制定出更加经得住考验和可接受的指导方针，各机构在标识脆弱性时可以此为参考，并对脆弱性矫正活动排出优先级次序。在这些指导方针广泛使用以前，联邦政府将努力强化其自身的信息系统安全操作规范和标准。

囿于技术和资金，所有的脆弱性都不可能同时得到立即矫正，在3~5年的时间内，基于对关键资产的标识和互依赖性分析，政府机构和私营部门将给这些矫正工作排出优先级顺序。详细的资金要求必须由首席基础设施保障官(CIAO)、首席信息官(CIO)和首席财政官(CFO)共同做出，然后由内阁成员或者首席执行官(CEO)和公司董事会采纳。

术语“一个互联网年”通常是指3个月。信息技术发展得如此迅速，以至于1年前采用的项目和计划与当前的新技术可能没有多少联系。随着网络的变化，新的脆弱性又会被引入。随着黑客对系统的不断揣摩，他们又会发现先前不为人所知的脆弱性。因此，我们要持续不断地评审新的脆弱性、新的保护措施以及新的操作规范和标准。我们要对技术变化导致的个别安全环节所表现出的脆弱性给予足够的重视。

由于对关键资产、共有的互依赖性和脆弱性的评估会给敌人提供攻击方法的蓝图，所以这些评估本身也要得到保护，要确保有合适的保护措施，包括可能的立法手段等（见内容9）。

联邦政府机构要持续地进行这种意义深远的风险和脆弱性评估，开发现实可行的多年度矫正计划。对这些评估和计划要做到持续地更新。同样，信息系统安全中的操作规范和标准也要有相应的更新。联邦各部局（PDD63在其中指定了基础设施部门联络官）将和私营部门共同合作，促进类似的评估和矫正工作的开展。

内容1时间表如下：

阶 段	行 动	目标日期
1.1	联邦一期机构完成最初脆弱性评估，制定矫正计划。ERT 将分析其报告	已完成 (1999 年 2 月)
1.2	联邦二期机构完成最初脆弱性评估，制定矫正计划。ERT 将分析其报告	已完成 (1999 年 5 月)
1.3	联邦各机构向 OMB 提交一份多年度的脆弱性矫正计划，同时提交 2001 年的预算，以后每年如此。ERT 将和各部合作执行其矫正计划	已完成 (1999 年 6 月)
1.4	CIO 委员会将成立关于联邦信息系统安全操作规范的一个跨机构工作组，它主要致力于确定、协调以及巩固正在开展中的政府安全操作规范制定活动。工作组将至少每年向 CIO 委员会做出安全操作规范的推荐报告。工作组还可以向 NIST 修订的联邦信息处理标准提出建议。NSA 和 NIST 将依据 1987 年的《计算机安全法》继续制定操作规范	已完成 (1999 年 11 月)
1.5	联邦政府将开发一个试验性框架及数据库，还包含若干实例，以获取并存储关键信息资产安全操作规范	已完成 (2000 年 1 月)
1.6	通过参照《PKI 组件最小互操作性规范 (MISPC)》，使联邦 PKI 用户和外部 PKI 成员用户之间的证书和 CRL 轮廓得到增强，以满足 MISPCv2 的主要管理要求；建立联邦桥 CA，加强 PKI 组件的互操作性基准，满足 MISPCv2 的保密性要求	2000 年 2 月
1.7	联邦政府完成关键物理基础设施保护计划的第 1 版	2000 年 6 月
1.8	关于操作规范的跨机构工作组将至少每年一次向 CIO 委员会提出有所推荐的新的或修改过的操作规范的书面报告。CIO 委员会将会对每一份报告进行发布，同时附上评论	2000 年 6 月
1.9	国防部关键资产拥有单位、国防基础设施部门的关键基础设施保障官以及设施和装备基地将确认其关键资产并执行初步的脆弱性评估。另外，国防基础设施 (DI) 部门关键基础设施保障官将执行部门级的脆弱性评价，确认关键的部门资产	2000 年 8 月
1.10	各国防基础设施部门和国防部关键资产所有单位将建立初步的方法和步骤，用于物理安全脆弱性评估、技术援助、认证和认可、人事安全事件及计算机事件	2000 年 8 月
1.11	联邦政府制定用来标识关键基础设施资产和互依赖性的方法	2000 年 9 月
1.12	国防部将完成其关键计算机系统物理保护的调查和评审，包括涉密和非涉密网络	2000 年 9 月
1.13	联邦各机构将确保软件补丁的实时安装以及其他计算机系统脆弱性矫正措施的实施。必要时，OMB 将监督这一过程的执行情况	2000 年
1.14	私营部门信息共享和分析中心将为会员公司开发一套用于评估和矫正项目的推荐方针	2000 年
1.15	国防部将更新其对关键基础设施保护项目的检查，以针对同关键计算机网络相关的基础设施的主要脆弱性而确定并推荐矫正意见	2000 年
1.16	私营部门信息共享和分析中心将评估各私营部门和工业界共有的脆弱性	2000 年
1.17	国防部将建立合适的组织结构来确认和矫正脆弱性，开发并配置入侵检测系统，开展重要的创新研究和开发项目	2000 年 11 月
1.18	国防部关键资产所有单位以及各部门关键基础设施保障官将提供矫正计划并为矫正计划提供资源。另外，国防部设施和装备基地将向部门关键基础设施保障官提供设施装备级的修复计划和资源	2000 年 11 月

续表

阶 段	行 动	目标日期
1.19	国防部关键基础设施部门关键基础设施保障官将监控响应活动，协调相关部门的减缓及重建活动，并为国家军事指挥中心（NMCC）提供支持	2000 年 11 月
1.20	DI 部门关键基础设施保障官将执行部门级的矫正措施，并整合和协调各部门内部资产级的矫正计划	2000 年 12 月
1.21	联邦机构应已经完成了信息系统脆弱性评估，采用了多年度资金计划来矫正这些脆弱性，创造了用于持续更新的系统。每一关键行业内的私营部门公司也应做到这样	2000 年 12 月
1.22	展示 PKI-Aware 应用程序的互操作性，如电子邮件，通过已出版的《证书发布及管理组件的安全要求》征求公众对 PKI-Aware 应用程序互操作性的意见	2000 年 12 月
1.23	不晚于 2001 年，联邦各机构应当在法律要求的范围内向 OMB 和 NIST 报告其对相关的安全操作规范和联邦信息处理标准（FIPS）采纳的程度	2001 年 1 月
1.24	关键基础设施保护整合工作组（CIPIS）将整合并协调国防部门级的矫正计划；评审国防部门的减缓计划和业务计划的制定；评审 DI 部门的重建计划；起草综合性的 DI 部门重建计划；起草各种有效性评测方案	2001 年 3 月
1.25	使用经签名的电子邮件：所有的电子邮件都将被签名，在整个国防部的范围内鼓励对邮件进行加密	2001 年 10 月
1.26	首次检验 PKI 组件对《证书发布及管理组件的安全要求》的满足程度	2001 年 12 月
1.27	国防部将向其所有 PKI 用户发行最安全的证书/令牌	2002 年 1 月
1.28	各国防部门将完成与基础设施依赖性和国家国防基础设施关键性评估有关的风险管理原则的制定和应用。完成这一任务将依靠：制定并实施一致的风险管理框架；确定风险和不确定性来源；确定因果关系；认识可能性和结果的影响范围；评估极端事件；考虑极端事件带来的风险；确定和分析各个可能的选项	2002 年 12 月
1.29	矫正计划应已经消除了联邦机构和主要公司的关键信息系统中绝大部分的已知脆弱性。脆弱性评估和矫正还要继续下去	2003 年 5 月

## 范围注解

### 保护计算机和物理关键基础设施

保护国家的关键基础设施长久以来就是政府关注的主题。水坝、桥梁、隧道、电厂和其他重要的物理建筑物已经被特别保护了50多年。1995年，PDD39指示总检查长负责开展了一次政府范围内的检查工作，以确定政府范围内的基础设施是否得到了足够的保护。

总检查长的检查突出显示了我们缺少对网络空间基础设施——关键信息系统和网络的保护工作的重视。这次检查的结果直接决定了总统关键基础设施保护委员会（PCCIP）的诞生。PCCIP发现了关键基础设施保护工作中的很多脆弱性，但却找不到任何系统和计划去解决这些脆弱性。

因此，总统在PDD63中阐述了他的意图：美国将消除那些被“针对我们的关键基础设施，特别是计算机系统的物理和计算机攻击”所利用的弱点。

为了重新研究非计算机系统的物理弱点，FBI、DoD和其他机构将评审1995年的工作，在必要的地方对这些工作进行更新，调整FBI的关键资产初步活动（KAI）和国防部（DoD）的关键基础设施保护项目。

一个新的《关键物理基础设施保护计划》正在开发之中，该计划将包含很多工作来确保对这些基础设施的保护。DoD、FBI正同CIAO合作，一起领导这个计划的开发。一旦完成，《信息系统保护国家计划》和这个新的《关键物理基础设施保护计划》就连接起来了，使我们可以采用横向的视点对其观察。本计划的第2版及更高版本会反映出这种横向视点。在将来，这两个计划可能会被合成到一起。

#### 内容 2：检测攻击和非法入侵

“今天，我们甚至不知道我们是什么时候被攻击的。”

内容 2 为我们敏感的计算机系统安装了多层保护，包括先进的防火墙、入侵检测监控器、异常行为标识器、企业级管理系统和恶意代码扫描器。为了保护关键的联邦系统，计算机安全运营中心（先是在国防部，然后是与其它联邦机构相协调的联邦入侵检测网络[FIDNet]）将收到这些检测设备发来的警告，也可以从计算机应急响应小组（CERT）或其他途径获得攻击警告，用来分析并协助各站点抵御攻击。

我们标识和矫正脆弱性的工作能够延缓但不能阻止对信息系统的恶意入侵。通用软件仍将继续具有脆弱性，不同软件和硬件组合中的相互作用也会产生出安全上的脆弱性。对系统有访问权的心怀不满的雇员会经常制造严重的破坏，他们的反常行为却可以长久地被人忽视，直到亡羊补牢，为时已晚。

考虑到系统和软件的脆弱性以及可能受害的目标系统的数量和非法入侵的频率，检测和监视系统的开发和使用是势在必行的。这些入侵检测系统已经在行政部门和国会中得到了应用。增强系统安全性的关键一步就是在整个联邦部门和机构中安装网络入侵检测监控器，并且要有一个能够对系统异常进行中央分析的功能模块。

社会生活中有很多警报器互联的成功例子。比如住宅报警系统——一个私人住宅遭到入侵时，当地警局的警报如果不会自动报警，私人防盗系统就会失去效果。

##### （1）安装入侵检测监控器和防御检测系统

检测网络中非法入侵行为的第一个必要步骤就是安装和使用高度自动化的应用程序，包括如下四类防御检测系统：

- 在防火墙两边安装的入侵检测监控器，该监控器要定期更新。
- 授权用户访问和活动的规则以及一个检测程序，以确定一个明显的授权用户所出现的异常行为。
- 企业级的管理程序，可以确认网络上有哪些系统，知道它们正在做的工作，还可以加强访问和活动规则并进行安全升级。
- 用来分析操作系统代码和其他软件的技术，以确认是否存在恶意代码（如逻辑炸弹等）以及其他类似于后门之类的危险代码（不论其初衷是恶意的还是善意的）。

本计划号召在联邦关键信息系统网络的如上四类防御检测系统中合适的地方安装同类产品最优程序。在政府内部，这些安装可能通过政府指令来完成。政府还可以通过信息共享和分析中心（ISAC）对这类系统做出评价（见内容 4）。

## （2）入侵检测监控器的网络系统

为了保护民事机构（非国防部）中的关键联邦系统，国家计划还要求将保护单个政府系统的防御检测系统和位于总务管理局（GSA）的 FedCIRC（联邦计算机事件响应功能中心）的中央分析单元联系起来。后者可以对多种网络的系统异常进行实时分析。如果联邦机构或者 FedCIRC 认为已经掌握了非法行为的足够证据，则将通知 NIPC，以进行下一步行动。只要任一站点受到攻击，有关攻击的警告词汇就可以立即引起其他站点的注意。

在目前的技术水准下，联邦入侵检测网络（FIDNet）以及其他网络监控系统需要自动感应和人工管理相结合。自动系统要求对政府网络内部关键节点上的系统异常数据进行有效收集。现在，系统异常分析在很大程度上依赖于各机构内的人工处理，一般由 GSA 的 FedCIRC 内受过专门培训的分析员来完成。随着研发的深化，越来越多的分析将使用人工智能工具来自动完成。此外，我们还需要有面对入侵时能迅速更新系统防御的自动化工具。

有三个系统共同支撑着美国政府的关键系统保护功能，FIDNet 将成为其中之一，具体如下。

- 国防部计算机网络防护联合特别任务中心（JTF-CND）：该中心已经建立起来，正在对国防网络进行监视，并可以在遭到入侵/攻击后对功能恢复行动进行协调。
- 国家安全事件响应中心（NSIRC）：为 JTF-CND、FIDNet 和 NIPC 提供专家帮助，协助他们隔离、控制以及解决危害国家安全系统的攻击和非法入侵。NSIRC 将和 JTF-CND、FIDNet、NIPC 一起协调对这些直接危害国家安全系统的攻击和入侵所做的事件报告和对脆弱性的评估。
- 联邦入侵检测网络（FIDNet）：是为了保护联邦民事部门的关键信息网络而创立的，它以国防部系统为模型，在 GSA 执行和操作。在法律的范围内，当非法行为的某些迹象需要得到 NIPC 的分析和预警部门的分析支持或者预警通知时，FedCIRC 将同 NIPC 进行协调。同样，当需要 NIPC 的计算机调查和执行部门的罪犯调查或国家安全调查时，FedCIRC 也将寻求与 NIPC 的协作。

司法部的预审认为，FIDNet 的理念同《电子通信隐私法》是相一致的。综合的法律评审（由各机构的代表实施）正在进行，以确保 FIDNet 在建设同政府的隐私和公民自由政策、法规及宪法的规定保持一致。

内容 2 时间表如下：

阶 段	活 动	目标时间
2.1	在空军、海军、陆军以及国防部建立连接入侵检测系统的分析及响应中心。建立国家安全事件响应中心（NSIRC）	已完成 （1998 年）
2.2	在关键性的国防部系统中安装第一批 500 套入侵检测监控器	已完成 （1998 年 12 月）
2.3	建立国防部范围内的 Hub（集线器），用于入侵检测系统——计算机网络防护联合特别任务中心（JTF-CND）	已完成 （1999 年春）
2.4	发布部级的计算机安全计划，在安全和应急处理办公室管理下重组能源部 CIO 办公室	已完成 （1999 年 9 月）
2.5	对联邦系统中的恶意代码进行初步的分析	2000 年
2.6	建立一个用于联邦民事机构的入侵检测网络（FIDNet）试点，到 2000 年 10 月要有 22 个关键性联邦网站连入	2000 年
2.7	对访问/活动监控进行升级，在联邦系统的合适地方建立企业级管理系统	2000 年
2.8	完成对具有自动化处理和可适应性功能的大型入侵检测网络上伸缩性（scaling）问题的处理以及其他事项的研发	2000 年 10 月
2.9	开发并定期升级入侵检测系统标准	2000 年 10 月
2.10	在联邦政府需要的地方对防火墙和入侵检测监控器进行升级	2001 年 1 月



内容 3：发展稳健的情报和执法功能以保护关键信息系统，保持与法律的一致

“人民组成政府是为了保卫人民，防御国外敌人和国内罪犯。”

内容 3 将帮助和加强美国执法及情报机构并转换它们的角色，使其能够处理计算机网络所面临的新型威胁和新型犯罪。

过去，国外对国内基础设施的威胁主要来自轰炸机、洲际导弹和潜艇。这些系统可以被情报机构定位和计算出来。但现在，我们的基础设施遭到的是基于计算机的攻击威胁，其危害度和来源很难被发现并估计。

依据行政令 12333、总检查长指导方针和中央情报局长的指示协议，美国情报机构最应该做的是收集国外信息战能力和意图的信息，这在所有的优先级中排第一。

情报机构要收集潜在的国外敌人的计划和攻击能力的信息，这是非常重要的。但是，收集计算机攻击威胁信息比收集传统军事威胁情报面临着更多困难和挑战。情报共同体正致力于开发新的解决方案，以应付这种艰难的挑战。

对计算机网络的攻击，无论是物理的还是计算机的，一般来说都违背了联邦或者各州的法律。要证明攻击已经发生、找到攻击者并证明其罪行需要新的技术，使执法、情报分析和国家安全响应能实现无缝结合。FBI 的国家基础设施保护中心（NIPC）是一个跨机构的保护中心，它使用来自多种资源的信息，包括开放资源、私营部门、执法和美国情报共同体，来提供攻击的早期警报，并通过收集在确定攻击方时所必要的信息，对攻击做出部分响应。而且，NIPC 还有执法和国外反情报使命，并在这些领域内的负责机关的领导和协调下进行运行。中心有来自国防部、情报部门、NSA 和其他联邦机构的代表。中心的角色是作为领头羊开发和改善一系列相关功能，用来判断入侵开始时间、分析攻击范围和攻击源以及寻找攻击者。

可能攻击的警告、适当的攻击事件和脆弱数据都将被私营部门、州和地方政府共享。这些信息对于提高它们的防御能力来说非常重要（见内容 4）。

通过其他项目的努力，美国执法机构正在提高和严格化国内的执法机制和工具。在司法部的计算机犯罪和知识产权处以及美国检查官办公室，我们都通过“计算机电信协调员”项目增加了受过技术培训的公诉官的数量，从而加强了对计算机网络罪犯的起诉能力。我们还与其他国家的可信执法伙伴进行了合作，以建立先进的国际合作系统，开发通用的方法以对非法入侵和计算机系统攻击进行定罪。

我们决心做到，任何滥用计算机技术的人，不论其是为了获取非法利益还是怀有其他邪恶目的，也不论他们这样做是为了国家、恐怖主义分子还是犯罪组织，我们都一定要找到他们并将其绳之以法。我们不会因为他们的罪行源于或超越了一个或多个外国的审判权限而放过他们。同时，我们还要开发与现有规则和政策相一致的很多其他政策和项目。这些政策和项目将主要关注国内执法部门和国家安全机构在各自的国内外行动中的法定角色。

内容 3 时间表如下：

阶 段	活 动	目标日期
3.1	提高联邦执法部门和情报机构对于收集、追踪以及分析计算机威胁和关键信息系统脆弱性的注意力	已完成 (1999 年)
3.2	情报共同体、国防部以及联邦执法部门发起一系列工作组，用于开发新技术，以完成信息收集和分析，对付计算机攻击带来的威胁	2000 年

#### 内容 4：以实时的方式共享攻击预警和信息

“攻击一点应视为攻击全体。”

1998 年 2 月第一次发现针对空军计算机的“Solar Sunrise”攻击时，我们还没有足够的措施和方法知道这些攻击是否也针对其他的国防部系统以及关键联邦网络或者关键私营部门系统。今天，已经有了初步的系统去做好这些工作。这篇国家计划要求建立一个更加有效的全国范围的系统来对攻击进行实时的信息传递，包括以下内容。

- 促进联邦信息共享：在当前的一段时间内，我们需要用手上已有的数据来完成更好的工作。联邦系统管理员有大量的关于异常和可能入侵的广泛数据，他们应该把这些数据发给 FedCIRC，包括 FIDNet 系统的增强功能模块。非法行为和入侵的迹象将被直接提供给 NIPC 分析。FedCIRC 还是重要的事件数据接收者和提供者。得到了所有这些资源的信息之后，NIPC 和 FedCIRC 将把这些报告同他们手头的其他信息结合起来，判断出入侵的模式或者那些貌似随机的事件之间的联系。

在国防部内部，国家军事指挥中心和 JTF-CND 将接收、巩固和评估国防部各部门的汇报；发现国防部内的入侵迹象并将其报告给 NIPC；发布国防部的预警；接收、评估和发布国家预警。

- ISAC：对于私营业主和州及当地政府，本计划鼓励信息共享和分析中心（ISAC）的建设。它将在公司和各州及当地政府之间共享信息，并接收政府的预警信息。有关 ISAC 和信息共享的白宫会议曾召开过，被 PDD63 指派为部门联络的几个联邦机构也曾主持过几个会议（包括前财政部长 Robert Rubin 和能源部长 Bill Richardson 主持召开的会议）。作为这一系列会议的结果，一些工业机构，包括通信和金融服务机构，已经决定建立 ISAC。其他工业机构正在评估这个提议。

NIPC 将向各 ISAC 提供威胁、脆弱性和相关事件的信息。

ISAC 以自愿的方式（对于那些愿意这样做的公司来说，绝对不是强制性的）把入侵和其他攻击信息通知给联邦各机构。发送信息之前，ISAC 可以预先对信息进行过滤（如删掉信息中包含的公司名称）。然而，我们提倡各公司直接向当地的 FBI 区域办公室报告计算机攻击事件。

#### 银行与金融部门 ISAC

1999 年 10 月 1 日，美国财政部长宣布开放银行与金融服务信息安全设施——金融服务信息共享和分析中心（FS-ISAC）。

该中心是一个公共-私营部门的合作项目，用来促进对金融服务业计算机攻击信息的共享。它为这些攻击信息提供了一个快速发布信息的匿名场所，提高了金融服务业对其技术基础设施受到的攻击进行防范、检测和响应的能力。

FS-ISAC 的成员资格向所有已获认可的金融服务协会的成员开放。目前，已有代表私营和公共利益的 12 个组织签署了信函，表明了它们对加入这个中心的兴趣。FS-ISAC 由私营承包商管理，并由各会员公司全额资助。

- 为信息共享排除障碍：很多公司可能希望同政府专家讨论可能的系统脆弱性，但又不敢这样做，因为根据《信息自由法》（FOIA），如果把信息透露给政府，那么同时

可能会被要求把信息向公众透露。关于政府脆弱性的敏感信息已经得到了现有法律的保护，不必因 FOIA 而向外泄露。为了促进这个国家计划，关键基础设施保障办公室（CIAO）和司法部共同召开了关于信息自由的 1999 年 7 月白宫会议，与会的还有公共和私营部门的专家。与会者讨论了 FOIA 对信息共享可能造成的障碍。通过私营部门的加入，一个跨机构工作组已经成立，其任务是推荐可能的全面解决方案。私营部门所关心的其他一些法律问题，包括反托拉斯和责任法等，也将得到类似的处理。

- FIDNet 和 JTF-CND: 在隐私和执法限制条例的许可范围内，FIDNet 和 JTF-CND 事件检测系统将在它们之间共享事件数据。
- 国家安全事件响应中心（NSIRC）: NSIRC 将从 FedCIRC 和 JTF-CND 获得数据，进行细致的事件分析和脆弱性评估。NSIRC 脆弱性评估将用于开发硬件和软件的计算机网络防御系统。

内容 4 时间表如下：

阶 段	活 动	目标日期
4.1	司法部和关键基础设施保障办公室（CIAO）在白宫会议中心召开一次关于《信息自由法》和保护关键系统脆弱性信息的会议	已完成 (1999 年 7 月)
4.2	在国家基础设施保护中心（NIPC）建立 24 小时全天候计算机攻击通知功能模块	已完成 (1999 年)
4.3	开发用于同私营部门的各个信息共享和分析中心（ISAC）进行安全信息共享的机制	2000 年
4.4	CIAO 和总务管理局（GSA）将为各联邦政府的 CIRC/CERT 发起一次白宫会议，推动这些公共运行系统的协调和发展	2000 年
4.5	提交法律方面的革新议案（如果需要），以帮助 ISAC 的建设	2000 年
4.6	同私营部门集团合作，在几个重要工业中建立 ISAC	2000 年及以后
4.7	在州一级上同多个州级权力机关一起创建“测试床”或计算机安全信息共享项目样板	2000 年
4.8	建立其他的信息共享和分析中心	2000 年

### 新墨西哥州关键基础设施保护委员会

保护关键计算机系统及物理基础设施的全州范围内的公共-私营合作样板

新墨西哥州关键基础设施保护委员会（NMCIAC）是一个私营-公共部门的合作机构，它的建立最初是为了商业团体、工业、教育机构、联邦调查局（FBI）、新墨西哥州政府和其他联邦、州和地方机构之间的信息交换，以确保对新墨西哥州关键基础设施的保护。NMCIAC 致力于研究威胁、脆弱性和对策，还针对基础设施攻击、非法系统入侵以及可能影响 NMCIAC 成员和（或）普通民众的那些因素所采取的各种响应进行研究。基于物理以及计算机的保护都是通过对关键系统的威胁信息进行参照和传播来完成的。在计算机和物理保护方面，NMCIAC 同 FBI 的 InfraGard/NIPC 活动结成了联盟。

NMCIAC 是美国第一个完全由自愿者组成的全州范围内的组织，为其他 49 个州内类似组织的发展提供了原型。在诞生后相对较短的时间内，它就招募了代表私营和公共部门

的 36 个组织。NMCIAC 使用工作组的形式完成其主张的目标。这些工作组依据不同的关键基础设施领域来定义：信息与通信；公用事业（天然气、石油、电力和供水）；银行与金融；运输；紧急事务管理；紧急情况和政府服务；信息共享和分析中心；管理和操作。

NMCIAC 定义了以下六个主要任务：

- 建立并管理以各州为基础的信息共享和分析中心（ISAC）。
- 创建并运行一个先进的安全通信系统。
- 确定并评估用来减弱威胁、响应威胁和事后恢复的技术。
- 发起并完成一个培训、推广、技术转让和技术协助项目。
- 开发并共享一个州级的关键基础设施保护模型。
- 管理和操作 NMCIAC。

为了迎接挑战并鼓励参加，NMCIAC 为其成员提供了很多利益：一个入侵报警网络；一个只为成员开放的信息提供网站；用来游说工业界做出必要改变和改善的工具；培训讨论会，帮助各成员完成其各自职责；各成员自己开发的项目，可以在各自的组织内分别执行。

对于那些有兴趣通过合作来保护其关键信息系统的其他工业部门和州及地方政府实体来说，NMCIAC 的成功是一盏指路的明灯。从 NMCIAC 中获得的经验能使社会的各个部门在关键基础设施的保障中受益。事实上，NMCIAC 官员正在同维吉利亚州官员合作，以期在该州开发一个类似项目。

### 信息共享和分析中心能为工业界做什么

国家计划号召工业协会或集团建立工业范围内的计算机安全中心，称作信息共享和分析中心，这些中心将做到：

- 在各公司间就脆弱性、企图的攻击和非法入侵的性质做到信息共享；这些信息可以被中心“过滤”，防止人们知道是哪个特定公司遇到了计算机事件。
- 协调工业界的特殊的研发需求。
- 检查整个工业范围内的脆弱性和依赖性。
- 开发雇员教育和意识培养项目；共享雇员培训项目。

### 政府怎样帮助信息共享和分析中心

国家计划号召政府通过如下措施对信息共享和分析中心进行协助：

- 提供重要攻击的实时数据，对网络面临的威胁进行战略性评估，提供攻击技术的信息，提供脆弱性信息。
- 协调联邦和工业界在信息系统安全方面的研发，帮助满足市场驱动力的需求。
- 为教育和意识培养项目提供资源及其他支持。
- 为了培养工业范围的 ISAC，对有关信息自由、责任和反托拉斯等问题的可适用法律做出必要的改变。

## 内容 5：建设响应、重建和恢复能力

“……对破坏进行隔离并使其最小化……迅速恢复必需的能力。”

内容 5 旨在攻击进行的时候对其进行限制；使相关团体和机构保持其职能的连续性；制定恢复计划，以对付信息攻击。

就其规模来说，信息战攻击可能不会限于一个个孤立的事件。它们可能是在一个整个的工业或机构内发动，也可能出现于一个完整的经济部门、国家的一个地区，或者是国家本身。通过使用 JTF-CND、FIDNet 和工业集团的 ISAC 所提供的攻击数据，NIPC 将和各联邦机构及私营部门合作，以确定正在发生的攻击的范围。

一旦一个大范围内的攻击得到确定，中心将与执法部门和其他机构协同工作，对攻击做出响应，包括向系统管理员建议执行一系列预定计划措施：

- 阻断可疑用户得以进入网络的通路。
- 实行特殊“防御状态”安全警戒。
- 针对攻击所采用的技术，应用新的安全软件“补丁”。
- 隔离网络的某些组成部分。
- 终止某些网络运行。
- 启用紧急事件下的接管系统。

与此同时，执法部门和其他相关机构将对攻击源进行定位并采取合适的措施将其中断。我们鼓励私营部门和执法部门之间关于攻击响应行动多做协商，以免私营部门的行动对入侵调查造成不必要的阻碍，防止抹掉入侵者的属性特征甚至耽误对侵略者的起诉。

政府的目标以及我们对工业界的建议是，每个关键性信息系统都要准备响应计划，这些计划中要包括为如下响应行动所做的准备：迅速启用其他的防御措施（如更为严格的防火墙要求）；在某些预定情况下关闭部分网络（通过企业级的管理系统）；把最小化基本操作交由“干净”的系统运行；迅速重建受感染的系统。

在很多情况下，企业和机构的恢复计划只集中于或主要集中于物理破坏：洪灾、暴风雪或爆炸等使总部瘫痪的事件。在这些计划中，作为替代的总部将接替原总部的运行，仍继续把各种指令发往各公司或机构的信息系统网络中。现在这些计划中通常包括“备份”计算机数据库，用于总部系统不存在或无效的情况。

如今，恢复计划还必须能够应付所有或部分信息网络本身被破坏的情况。这时，一定要有替代的方法用来传送最小量的重要信息。专家组要立刻赶到以协助重建工作，包括分析导致网络瘫痪的软件错误以及设计替代方案等，还要负责网络重启。

在这个世纪之交，我们有可能遇到同 Y2K 有关的崩溃事件，可以创建 Y2K 信息协调中心来协调事件信息流。这个中心由政府 and 工业界的专家联合组成，并和国家信息中心（NIC）的系统合作。后者的职责是收集各部门的状态信息。

在 PDD67 中，总统指示每个联邦部门和机构在 1999 年底以前提交确保运营连续性的计划。这些计划要含有在 PDD63 中所述的任何紧急情况发生时确保运营连续性的措施。

联邦部门联络官将同各自对应的工业界合作，确保企业的恢复计划中也同时提及了信息攻击的重建。商务部内跨机构的基础设施保障办公室（CIAO）将发起一次有保险业和审计业代表参加的白宫会议，并同他们开展持续的对话，以促进对风险管理、操作建议以及衡量标准的理解。

内容 5 时间表如下：

阶 段	活 动	目标日期
5.1	各部局将修改其运营连续性计划，考虑进意外事件以及 PDD63 中谈到的紧急事态	已完成 (1999 年 12 月)
5.2	关键基础设施保障办公室（CIAO）将发起一次有审计和保险业代表以及部门协调员参加的白宫会议，会议集中关注商业控制和审计界在信息时代的新角色	2000 年
5.3	JTF-CND 以及其他政府机构将为政府的信息攻击预警网开发协议和建议	2000 年
5.4	联邦应急管理局（FEMA）将进行应急通信系统的现代化改造	IOC：2000 年 FOC：2003 年

内容 6：为支持内容 1～5，加强研究和开发

“信息技术正以互联网年的速度发展着，1 个日历年的时间相当于 4 个互联网年。”

第 6 项内容系统地确立了实现这个计划所必需的研究要求和优先级顺序，确保了这些研究的资金来源，而且，该步骤中还建立了一个系统，用来确保我们的信息安全技术始终紧跟整个信息系统中的威胁的变化。

只依赖现有的技术，本计划前 5 步所要求的很多任务是无法有效开展的，甚至有些情况下全然不能执行。跨机构的关键基础设施协调组（CICG）已经建立了一套步骤来确定这个计划的技术要求。由科技政策办公室（OSTP）领导，研究和发​​展子工作组将与各机构和私营部门合作，以实现：

- 就信息安全研发的要求和优先级取得一致意见。
- 在联邦各部局中进行协调，确保各部门的研究预算要求得到满足，防止部门工作的浪费和重复。
- 与私营部门和学术研究员交流，防止联邦资助的研发与私营部门及学术界以前的、正在进行的和将要进行的计划发生重复。
- 确定在信息安全技术中，市场还没有投入足够或充分的研究工作的领域。

该过程始于 1998 年，在 2000 年的行政预算中，这些基础设施保护研究将花费 5 亿美元。这一过程中确定的优先研发的项目为：

- 支持大规模入侵检测监控网络的技术。
- 能够确定操作系统代码中恶意代码（陷门）的人工智能技术及其他方法。
- 在攻击或灾难中能够控制、阻止和驱逐入侵者并减弱破坏程度或恢复信息处理服务的方法。
- 可以增强网络可靠性、系统生存力、关键基础设施组件和系统乃至关键基础设施本身的稳健性的技术。
- 对基础设施响应进行建模的技术；确定互依赖性及它们的影响；定位主要的脆弱节点、组件或系统。

CICG 的 R&D 子工作组在 1999—2000 年发起一系列会议。

CIGG 的 R&D（研发）子工作组正在发起很多讨论组来研究那些受关注的、横向的研发主题，包括：

- 入侵、恶意代码和异常行为检测（1999 年 2 月 22 日—23 日）；

- 关键信息系统基础设施间的互依赖性（1999 年 8 月 11 日—12 日）；
- 恶意代码（时间待定）；
- 内部人员威胁（时间待定）；
- 入侵检测（时间待定）；
- 重建/恢复（时间待定）。

内容 6 时间表如下：

阶 段	活 动	目标日期
6.1	协调联邦政府关键基础设施保护研发工作，为 2000 年及后续财政年度的预算做准备。确定国家计划执行中需要的研发项目，制定多年度的资金战略，并把第一年的资金要求纳入 2001 年度部级预算需求之中	已完成 (1998 年 6 月)
6.2	在向私营部门和学术界的咨询下，科技政策办公室（OSTP）将每年更新联邦政府关键基础设施保护研发项目中的优先级	1999 年 9 月 由此继续
6.3	召开有工业界、学术界代表和政府专家参加的会议，讨论研发项目的优先权，建立公共-私营机制来协调联邦和私营部门对关键基础设施保护的研发，协调内容 7 中人力和培训方面的工作与资源，建立并支持培训方面的研发，使本科生和研究生具有熟练的技术	1999 年 12 月 由此继续
6.4	确定国家计划所需的主要研究项目的成功日期	2000 年 1 月
6.5	对创建中央 R&D 联邦基金进行评估，以对横向项目进行支持，确保 2002 年及后续年度预算中公共-私营研究的协调	2001 年 3 月
6.6	建立信息基础设施保护学会，对各类研究项目进行资助	2001 年

内容 7：培训和雇佣足够数量的信息安全专家

“我们所没有的恰恰是经过专业培训的人。”

内容 7 概览了联邦政府和全国范围内信息安全专家的数目和所需的技术，采取措施来培训现有的联邦 IT 雇员，并征募和教育其他人员来弥补这种人才的亏空。

有证据表明，在全国范围内，我们面临着熟练的 IT 人员越来越供不应求的危险。尤其是在信息系统安全人员这一子集里，这种状况更加严重。在联邦政府内部，熟练的信息系统安全人员的缺乏也发展成了一种危机。雇员的匮乏反映了大学研究生和本科生的信息安全课程实在太少。为了解决这些问题，我们将调节并依靠国防部、国家安全局、CIO 委员会和各种联邦机构的工作。

FCS（联邦计算机服务）的培训和教育活动引入了以下 5 个项目来帮助解决联邦 IT 安全人员缺少的问题。

- 完成人事管理办公室 IT 职位研究：该研究将有助于确定联邦政府内 IT 职位的数量、这些职位所要求的主要能力以及这些职位所需的培训和认证。
- 发展信息技术优秀中心（CITE）：这些中心将培训和认证现有的联邦 IT 人员，帮助他们在整个职业生涯中维持其技术水平。这些中心还将吸取国防部和其他联邦机构在这个问题上的重要项目成果。
- 创立 SFS（服务奖学金）项目，从而招募和教育下一代联邦 IT 雇员和安全管理员：这个计划将每年资助 300 个学生，帮助他们完成在信息安全领域的本科或研究生学业。作为偿还，学生在毕业后将在联邦 IT 岗位上服务一段固定的时间。计划还将

包括一项很有意义的暑期工作和实习内容。SFS 项目的一项主要工作内容是确定参与项目的大学，并对这些大学里的信息安全职员和实验室发展进行帮助。

- 发展高中招募和培训活动：这一项目将确定出有潜力的高中生参加暑期工作和实习，使他们熟悉联邦 IT 工作标准，为将来到联邦 IT 岗位就业做准备。该项目还将检查那些旨在提高中学生计算机安全意识培养的可能方案。
- 开发并使用联邦 INFOSEC 意识培养课程：该项目旨在确保整个联邦岗位都在发展计算机安全意识教育。它将利用几个杰出的联邦机构意识培养项目。

内容 7 时间表如下：

阶 段	活 动	目标日期
7.1	展开大学中的推广工作，以推动 SFS（服务奖学金）项目的发展。对 SFS 候选人进行认证，建立专题讨论会以招募可能的候选人。如果需要，为任何其他权威项目制定提议	2000 年 1 月
7.2	对联邦范围内信息系统安全培训和教育项目进行完整的评审，确定现有的培训和教育项目，找出任何差距或冗余	2000 年 3 月
7.3	为申请并入选 SFS 的项目制定标准、备案要求和指导方针	2000 年 4 月
7.4	利用国防部和私营部门的模型，开发联邦 IT 安全雇员认证项目，用于系统管理员和各 ISSO（信息系统安全官）；开发培训项目，用于满足这些认证目标的需求	2000 年 5 月
7.5	开发并传播联邦岗位 INFOSEC 意识培养课程。各 CITE（信息技术优秀中心）中的一个将负责这一项目，预先审查和更新其内容	2000 年 5 月
7.6	制定指定 CITE 时的标准	2000 年 6 月
7.7	设计和执行中小学推广计划，包括各种会议、暑期工作和实习	2000 年 7 月
7.8	任命参与第一年 SFS 项目的一批大学	2000 年夏
7.9	在联邦政府内完成由 OPM（人事管理办公室）领导的对信息系统安全职位需求的研究。这将为联邦 IT 岗位的人员招募、推广、选择、工资偿付和能力发展提供可靠的数据	2000 年夏
7.10	为未来的 SFS 教职员开展一个试验性的信息系统培训项目。这将成为我们的教职员发展项目的前导	2000 年夏
7.11	为 2001 年开始的第一年 SFS 项目招募研究生和本科生，以后每年招 300 个学生	2000 年秋
7.12	确定、指派各 CITE，并为其提供资源。中心将为联邦 IT 雇员开发和提供高质量的信息系统安全培训及认证；还向 SFS 和暑期工作项目中的中学生提供技术认证和培训项目	2000 年 10 月
7.13	第一批 SFS 项目学生开始学习	2001 年 1 月
7.14	SFS 计划的第一批研究生进入联邦 IT 工作岗位	2002 年 5 月

内容 8：加强推广，使美国人民知晓加强信息安全的必要性

“知前行后。”

第 8 项内容向公众解释现在就采取行动的必要性，在灾难性事件到来之前，提高我们防御处心积虑的计算机攻击的能力。

保卫美国的网络空间需要所有美国人——商业领袖、教育和其他私营机构、政府（联邦、州和地方）以及普通公众都行动起来。作为国家计划所阐述的很多行动的基础，我们要对信息系统所面临的新威胁以及行动的必要性具有一定的理解和认识。



到目前为止，还没有“电子珍珠港事件”来唤起公众对行动必要性的认识，也没有太多的美国人领会到我们的经济和国家安全对计算机和信息系统的依赖程度——这些系统的功能通常被日常生活隐蔽掉了。

结果，我们不得不做很多意识培养方面的广泛工作。在初始阶段，至少有以下 3 项工作要做：

- 通过计算机公民项目，对美国儿童进行计算机道德和正确使用互联网及其他通信工具的教育。
- 通过关键基础设施安全合作组织（PCIS）项目，打造美国企业领导和信息技术领导的合作联盟。在这个项目中，我们都认识到了在私营部门和政府中采取特别措施以提高我们国家的计算机安全的必要性，并在全美范围内认可的项目中实现合作。
- 确保联邦雇员本身能够意识到信息系统安全的必要性。

过一段时间，还将加入第 4 项工作：

- 基于以上的工作，把我们的意识培养活动扩展到其他私营组织和普通公众中去。这些行动构成了我们保卫美国的信息基础设施的基础。

内容 8 时间表如下：

阶 段	活 动	目标日期
8.1	通过创建计算机公民项目，对美国儿童施以使用计算机系统时行为正确和道德方面的教育	已完成 (1999 年 5 月)
8.2	通过创建公共-私营关键基础设施安全合作组织（PCIS）项目，提高各公司及政府对关键信息系统和计算机网络所受威胁的认识	2000 年 2 月
8.3	向所有可以接触敏感信息系统的联邦政府人员提供强制性计算机安全意识通告。这种强制性通告在他们一接触其业务时就要提供，并且以后至少每两年提供一次	2000 年 3 月

内容 9：采用立法和拨款手段，支持内容 1~8

“正如政府必须和私营工业形成合作联盟一样，行政部门和国会也必须紧密合作，共同保卫我们国家的关键基础设施。”

第 9 项内容为支持其他内容提出的活动提供了法律框架。这个活动要求联邦政府内部，包括国会同私营工业紧密合作。

总统已经提出了一些行动建议，并指示：联邦各部局要努力确保自身关键系统的安全，还要同私营部门建立合作联盟以保护我们国家的基础设施。很多类似活动得到了国会的支持，包括在 2000 年预算中拨款 17.37 亿美元。

国会议员和各委员会的行动表明，他们也意识到了我们国家的关键计算机系统所面临的潜在攻击威胁，而且他们还预先采取了很多保护性措施。我们正在评审现有的法律以及先前引入的立法提议，并正在为提高关键基础设施安全性制定很多新的提议。

正如其他项内容中所述，我们需要新的法律以建立工业和政府合作的基石。为了推动私营部门信息共享和分析中心（ISAC）的建设并促进私营部门和政府间的信息共享，在涉及同私营部门共享信息的事务时，我们必须有能力保护敏感的信息并缓解潜在的责任和反托拉斯问题。

为了确保这篇国家计划中某些行动的有效开展，我们正在调查建立新的法律机构的必要性。我们时刻考虑着保护公民自由和隐私的绝对需求，因此将制定出法律框架来提高保护关键系统的全面运行能力。我们需要国会支持总统为内容 1~8 所划拨的预算资金。国家计划中各个时间表内的任务的成功实现也依赖于资金提供的级别。

我们期待着继续和国会进行建设性的对话，讨论保护关键系统的最好的方法和机制，并敦促其积极参与这个国家计划未来版本的制定。

内容 10：在计划的每一步骤和每一部分中，要确保美国公民的自由权、隐私权和私有数据保护权得到全面保障

“……人民的人身权、不动产权、著作权和财产权应该得到保障……”

第10项内容与其他几项融为一体，它确保我们在保护关键计算机系统时的所作所为都符合宪法和其他法律的规定。

保护我们的关键基础设施是很重要的，但保护公民的自由同样重要。国家计划中所有的提议与现有法律和隐私期望完全一致。这篇国家计划要求每年召开一次关于计算机安全、公民自由和公民权利的公共-私营讨论会，以确保国家计划的执行者始终关注公民的自由，并且其计算机安全提议要由政府内外的民权专家和感兴趣者进行讨论。

国家基础设施保障委员会（NIAC）由来自联邦政府之外的参与者组成，它也将每年对计划执行中有关公民自由权、隐私权、私有数据保护权的活动进行审查。

国家计划在设计时融入了《法律第四次修正案》规定的隐私保护要求。政府检查公民计算机或电子通信内容的任何举动必须与现有法律，如《电子通信隐私法》相一致。公民同敏感性的政府资产，包括政府 Web 站点打交道时，应该被明确告知对他们行动的监视是否是他们能够访问这些资产的先决条件。国家计划要求建立一个相关系统来确保所有受监视的敏感资产都向访问者提示了必要而清楚的警告。

美国政府已经开始了同私营部门的合作，为隐私保护制定强制性规则，以确保 Internet 用户已被明确告知他们的哪些个人信息已被他人收集以及这些信息将做何种用途。要给用户提供服务，由他们自己决定其个人信息的用途，从而确保其数据的安全，为合理访问信息提供条件。还要给他们提供求助机制，当他们的个人信息被非法滥用时能得到帮助。

内容 10 时间表如下：

阶 段	活 动	目标日期
10.1	联邦政府与政府外的组织合作，举行每年一次的公共-私营计算机安全、公民自由和公民权利讨论会	2000 年
10.2	NIAC(国家基础设施保障委员会)和其他相关的权威机关将针对公民自由、隐私权和私有数据对国家计划的执行情况进行年度评审。另外，还将评审政府和私营部门的其他相关活动以及政府对私有数据的处理，以推动更为广泛的信息共享	2000 年

## 1. 美国关键基础设施面临的威胁

我们面临着很多危险。当今的美国比以前任何时候对计算机的依赖性更为强烈。但是，我们设计计算机安全软件、培训信息技术安全人员、开发和推广计算机安全操作建议和标准

的能力已经远远落后于对每一关键基础设施进行计算机控制设备安装所需要的技术驱动步伐。我们的国家安全和经济稳定性已经非常脆弱。这不仅会影响电力、通信以及任何公共事业中的计算机控制系统，还会威胁到保存医疗数据、犯罪记录以及财产信息的重要数据库。在惹是生非的黑客、硬件和软件缺陷、计算机犯罪以及更令人担忧的敌对国家和恐怖分子的处心积虑的攻击面前，我们实在是脆弱不堪。

让我们看看以下事件：

- **Kansas** 上空的通信卫星失控，超过 35 000 000 美国人的寻呼机停止工作。
- 某一大区域内的电话服务被切断，造成一个重要地区机场内的所有联系中断，威胁到航班的最后着陆。
- 美国两个最大城市的 911 服务瘫痪，引发混乱，所有救援行动因此而变得迟缓，并导致了可能的异常死亡。
- 1998 年 2 月中旬与伊拉克的冲突中，发现了针对陆、海、空三军以及国防部后勤和计算机保障系统进行的大范围入侵。我们并不知道入侵源于何方，也不知道入侵已持续了多长时间以及哪些信息遭到了窃取和篡改。
- 一种新的计算机病毒在互联网上正迅速扩散，通过寄发大量的电子邮件使系统过载，导致很多公司和政府系统被迫关闭。

所有的这些事件都是真实发生的，不是在同一天，也不都是美国的敌人有预谋行动的结果，但是都发生在过去的 36 个月内。如果美国政府正面临外事政策的挑战、准备部署外交人员和军事力量并且这些入侵事件恰恰都是由我们的敌人发动的，而且是他们的最后通牒，在这种情况下，让我们想想这将引发的一切商业和政治后果吧。

这些计算机入侵、攻击以及系统脆弱性举目皆是，包括我们的军事、政府及民用基础设施，它们中没有哪个能幸免于计算机网络攻击。

- 国防部副部长 Dr. John Hamre 最近证实：“这个世界正变得越来越不太平，我们已经提高了对网络活动进行监控的能力，可以观察到的探测、入侵行为和其他计算机事件的数量持续增长。目前我们每天能检测到 80~100 起事件，其中约有 10 起需要做进一步的调查。”
- 1998 年，一家电信公司在其 Internet 接口处安装了一个入侵检测系统，每月约发现 4 000 次入侵尝试。尽管大部分是无害的扫描，但其中也有数百起是攻击性的，这些攻击试图侵入其数据库并转移电话卡上的金额。
- 1998 年，一个民航公司对其计算机系统的脆弱性做了一次评估。模拟攻击中，作为攻击方的红队能够破解其 90% 的业务，并可以访问其工资数据，更为危险的是，红队甚至能够侵入航班数据录入程序。
- 为抗议美国 1999 年 3 月的军事行动，有人对 5 个联邦非国防机构的计算机系统同时发动了攻击，攻击手法是利用 E-mail 炸弹或修改及破坏主页。

自 20 世纪初开始，摧毁或破坏为军事力量提供支持的通信、供给和经济基础设施就成了一条重要的军事原则，被认为同攻击军事力量几乎同等重要。从传统意义上讲，美国位于我们的对手所能作用到的物理范围之外，而计算机时代的到来则为我们潜在的对手提供了全新的选择。我们的基础设施正处在 10 年前看起来还遥不可及的攻击方式的危险之中。

国家依靠互联的信息系统来执行电信、能源、运输、经济和国家安全职能。但这些网络在由技术天才群体发起的破坏和入侵面前非常脆弱，且少有例外。作为美国敌手的主要攻击目标，这些网络正面临着越来越大的危险。商业网络所面临的危险比起政府网络来只多不少。

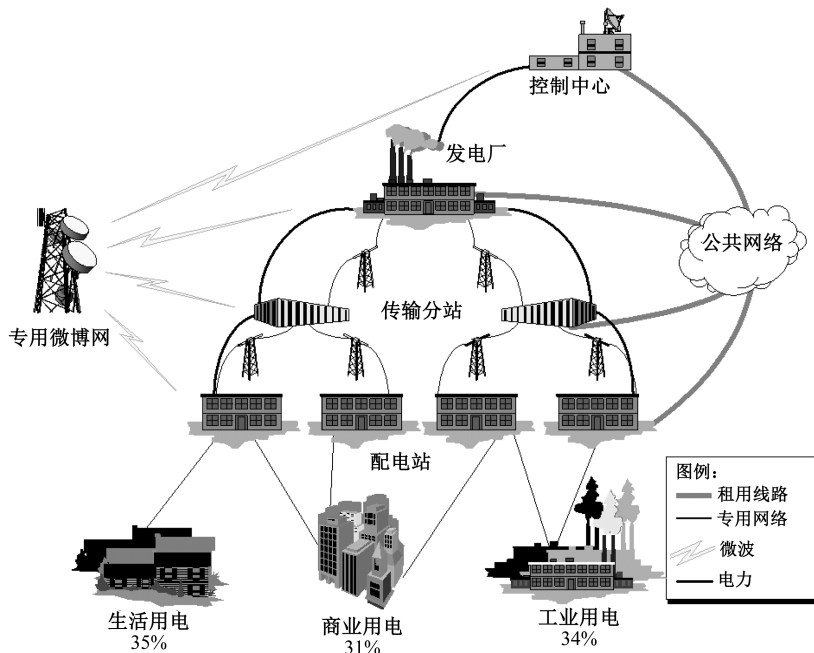
我们可以现在就行动起来进行自卫，或者等到事故发生并引起注意后再采取措施。但是如果延误了时机，日益增长的系统依赖性、越来越多的脆弱性和危险最终将产生非常严重的后果；而如果我们立刻行动，情况则会好得多。

### 日益增长的系统依赖性

美国正率先建设并全面发展信息经济。制造商、金融机构、运输商、不计其数的其他商业机构以及联邦、州和地方政府都在全力建设信息网络，以提高效率、降低成本或开发新型业务。

例如，生产商和提供商现在可以使用电子连接实现面向消费者实时需要的产品生产，从而降低生产成本。电力和通信业务提供商已把他们的控制系统进行了互联和内联，可以提供更加快捷而廉价的服务。计算机互联网在能源、水利、金融服务和运输服务的控制中已经得到了普及性的应用。各级政府也靠这些网络和基础设施来提供基础服务。

没有哪种基础设施比电力更能积极地促进计算机的变革。更重要的是，电力基础设施是国家其他所有基础设施的血液，因而它的安全和保障是我们的国家安全和经济稳定的关键，并且，它对于应急医疗、消防和警务服务也非常重要。电网上的任何脆弱性都必须得到详细确认并完全改正。电力系统框架如下图所示。



通过信息网络，商界和政府可以获得显著效益并开拓新型服务。但是，在这场技术变革中，我们曾对技术发展做了不理智的决定，使公司和国家对这些系统特别依赖。国家的经济

力量、众多的商业利润和生存能力以及联邦政府的职能运行现在都极大依赖于这些复杂网络的运行可靠性。

**信息网络的大量脆弱性**

对很多网络系统所采取的有预谋入侵只需要低廉的成本和很少的时间，且非常容易。我们的信息基础设施的很多脆弱性在入侵者中广为人知，他们可以通过互联网和其他途径共享这些信息。很多强有力的攻击方法可利用设计精巧的程序自动完成，在 Internet 上很容易获得计算机窃贼工具套件。任何意欲攻击我们的信息基础设施的人，只需要在设备上投入极少的资金、掌握中级水平的技术能力、拥有一套容易组装的工具以及了解一些可以从网上或其他开放资源处获悉的系统脆弱性和攻击技术，就可以轻松完成对这些基础设施的攻击。

计算机入侵者面临的风险极小。不同于攻击物理性基础设施，对信息网络的计算机攻击不需要物理上的接近。攻击可以来自世界上任何地方，通过互联网、其他网络和拨号线路中的一种或几种的组合来施行。经由多个通信网络和计算机链发动攻击，入侵者可以有效掩盖其身份和位置，追踪这些攻击却非常困难且耗时极多。

计算机入侵者能够轻易地采取声东击西战术来隐藏其真实意图，从而达到预期的效果。入侵者可以使用病毒、网络蠕虫、特洛伊木马、计算机时间炸弹以及其他自动攻击方式来轻松使成千上万的组织和网络陷于瘫痪。计算机入侵者可通过这些行动将系统和网络操作员、安全事件响应小组以及事件调查组的注意力从其真实攻击目标上转移开。当背景噪声达到相当的程度时，对关键系统的攻击可以变得神不知鬼不觉。

“像美国这样一个高度计算机化的社会，对于来自各个层面的电子攻击表现得极端脆弱。这是因为美国的经济，从银行到电话系统……都完全依赖于计算机网络。”——某外国政府报纸。

信息时代威胁图如下：

国家安全威胁	信息战士	减小美国决策空间及战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	恐怖分子	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

**日益增长的危险——数目正在增加的潜在计算机攻击者名单**

今天，对基础设施发动一次攻击所需要的条件可能只不过是一台个人计算机以及相关使用技术。我们的高精度、多用途的情报装备虽然可以监控复杂的大型军工综合设施，但我们的敌人却不需要去操作这些被监控的设施。对我们的攻击可以来自任何地方的一台计算机——在敌对国或是友邦，甚至就在美国境内。这些怀有恶意甚至敌意企图的攻击试图以电子方式阻止我们访问关键性信息网络，阴谋通过控制或改变我们的信息系统来达到对我们进行欺骗的目的，或进行传统间谍及经济谍报活动。

美国的对手分布广泛。从 20 世纪 70 年代开始，我们就了解到一个沉痛的事实：我们的某些敌人有时是非国家组织，包括恐怖分子、毒品贩子和国际罪犯。他们对美国的政策、目

标和价值观念持反对态度并且不以外交方针和军事对抗的形式来表现。针对美国基础设施进行成功的计算机攻击是他们采用的一种不错的方法，而且很适合他们的口味和目的。

### 国家威胁

我们知道几个正发展信息作战能力的国家。显然，并非所有这些项目都已达到了成熟阶段，但据情报部门预计，这些国家可能正在开发侵略性的计算机网络应用（CNE）和（或）计算机网络攻击（CNA）能力。尽管很少有人公开谈论他们的这些开发工作，但是在一些国家的公开出版物上可以看到他们对 CNA 价值的讨论。

“一个想要对美国进行摧毁的敌手只需要用先进的技术扰乱银行的计算机系统，就可以损害和破坏美国的经济。如果我们忽视了这一点，只是单纯依靠建立一支耗资巨大的常备军队，那简直就如同建造可笑的马其诺防线。”——某外国政府报纸

我们也知道一些国家的信息战计划是特别针对美国的。潜在的敌人将会攻击美国的关键基础设施以达到如下三个主要目标之一：在与美国对手的竞争中协助该国政府所投资的公司获利；攻击我们的金融或工业资源，以破坏我国的经济稳定；发动军事或情报活动，破坏国家安全。

“在适当级别上保持我们核威慑潜力的同时，我们必须对全面的信息战投入更多的注意。”——某外国政府首脑

### 经济竞争者

据克林顿总统的《关于外国经济情报收集和工业间谍向国会提交的 1998 年年度报告》，已有为数不少的国家盯上了美国的工业和经济信息。不仅仅是官方情报机构参与了谍报活动，一些外国主要的工业部门也在其国家商业情报工作中发挥了主要作用。他们瞄准美国民众、工厂、工业和美国政府，偷窃先进的关键技术、贸易秘密、财产信息以及研发成果，这种威胁长久以来一直存在着。

### 犯罪分子

计算机犯罪活动给美国公司造成了巨大的经济损失。信用卡公司、电话公司以及金融机构都在这样一个计算机犯罪激增的大环境下进行运营。*Ernst and Young/Information Week* 的一次调查表明，在过去的 5 年内，超过 72% 的美国公司发现它们的数据正面临着不断增长的安全威胁。

国内和国际上有组织的犯罪集团正日益引起美国执法部门的密切注意，并且在世界范围内都成了执法机关的关注对象。这些犯罪集团借助于高科技用于各类目的，不只为了获得经济利益和竞争优势，还试图获取警务计算机和网络中保存的敏感性执法信息。

很难估计美国公司受到攻击的程度。某些情况下，甚至无法对公司的损失程度做出明确认识，而且，有的公司还对事件保密，因为它们担心由此造成的负面影响。1996 年，参议院少数人报告<sup>①</sup>恰如其分地揭示了大多数公司的想法：

---

① 指在一次调查后由少数人做出的报告，一般与多数人意见相左——译者注。

“由于害怕影响顾客或持股人的信心,商务部门不愿意报告计算机入侵事件。一般情况下,公司内的人士可能向职员透露他们已遭受入侵的消息,但不会将事件报告给政府和其他机构,因为他们担心这些事件进入公众视野。”——参议院少数人报告“网络空间的安全”听证会。

## 黑客

曾经,黑客是那些十多岁的计算机天才和极度狂热的程序员,他们并不热衷于犯罪或恶意行为,他们的行为被认为是受好奇心和挑战欲望所驱使。不幸的是,新一代黑客看起来是受贪欲或恶意所鼓动的,而不再是简单的好奇心。黑客已开始认识到计算机系统的信息的价值以及他们可以通过盗用通信服务、进行计算机欺骗获得的潜在利益。如今的黑客们出于各种各样的原因而向程序中插入恶意代码、发动拒绝服务攻击,包括贪欲、政治目的、偷窃信息或者只是简单的恶作剧,而且,他们对计算机系统造成严重破坏的能力已经有了显著增强。

### SOLAR SUNRISE

**事件:** 国防部计算机系统遭到有组织的黑客攻击。

**时间:** 1998 年 2 月 1 日至 26 日。

**人物:** 在一名以色列青年协助下的两位 16 岁加州男孩。

#### 攻击:

- 攻击国防部网络域名服务器,利用了已广为人知的 SOLARIS 操作系统的弱点;
- 分布广泛;
- 经过细致协调;
- 攻击国防部未加密的网络的关键部分,包括全球传输系统的支持系统、国防部金融系统、医疗、人事、后勤设施以及未加密的官方电子邮件;
- 获取了很多口令。

#### 教训:

- 预警系统有待改进;
- 入侵检测系统有所提高,但仍不够;
- 政府组织方式上存在缺陷,司法部 (DOJ) 与国防部 (DoD) 的关系不够明晰;
- 在对攻击进行特征化并提取攻击属性上存在问题;
- 需要建立常备响应队伍;
- 需要在培训和人力方面进行投资。

**结果:** 三人被逮捕;其中两名美国人被起诉并因 SOLAR SUNRISE 入侵被判罪,第三人的起诉要在以色列进行,待决。

## 恐怖分子

在过去,恐怖分子一直想方设法通过对非军事目标进行暴力活动来对公众造成影响。恐怖分子的传统定义是那些系统化地使用暴力手段向政府或社会进行恐吓或施压的人,他们的典型手段是爆炸或攻击那些外观巨大或能引起媒体热切关注的目标,恐怖组织所反对的政府或意识形态的象征物也是恐怖主义分子热衷的目标。然而,信息战技术的出现为恐怖组织提供了更为强大的恐吓或混乱制造工具。

美国空军提供的一份最新报告详细描述了恐怖分子对计算机工具日益采用的情况以及这种趋势对美国造成的威胁。

“网络的兴起可能重塑了信息时代的恐怖主义，使其可能采用网络战——信息时代中一种由非国家机构占主导地位的冲突。”

“激进而活跃的新一代人，正在开始建立信息时代的意识形态。新型势力，如无政府主义者和虚无主义者的计算机团体，也有可能参与到网络战争中来。”

“在非对称冲突中敌人处于有利地位，因为在网际空间中没有人可以占据统治地位，权力或政府部门有可能处于最低的知识水平上。”——RAND 公司

已经发生过好几起引人注意的恐怖主义组织行动，包括 1997 年泰米尔游击队发起的“Internet 黑虎”拒绝服务攻击，在整个欧洲、北美洲和亚洲，对 Sri Lankan 计算机进行了为期两周的攻击。

### 内部人员

“1988 年 4 月，一名心怀不满的雇员引爆了一颗逻辑炸弹，破坏了新泽西工程工厂控制其生产线操作的计算机文件。这颗逻辑炸弹不仅使公司的运行陷于瘫痪，还破坏了工厂的备份计算机文件。由于没有能力完成恢复或重建，这家工厂最终破产。”——多篇新闻报道

内部人员对信息战中各种组件的熟悉使这些组件变得极为脆弱。内部人员最终可能是对我们的各类关键基础设施——军事设施、联邦设施以及民用设施的最大威胁。内部人员通常对组织的文化理解得最为透彻，并非常了解基础设施及其支持系统的操作。心怀不满的工人、被收买的告密者、被欺压或是被伤害的雇员、以前的雇员以及商业合作者都有可能被鼓动去计划或实施攻击，原因不一而足，如报复或经济目的等。恶意的内部人员可能单独行动，也可能与企图攻击基础设施的外界个人或组织合谋。

### 总结

不幸的是，我们有史以来的防御和情报投资对预测甚至检验我们的联网系统所受到的计算机攻击帮助甚微。我们的国家情报机构有能力“看到”军队和军事设备的调遣，“感觉到”导弹发射或其他活动，“听到”潜艇或指挥控制通信系统的声音，但它们并非为检测计算机攻击而设计的。

有必要认识到，不仅仅攻击国防部和情报共同体的计算机会带来危险。太多的部门中存在着大量弱点——大部分在私营部门，它们将首当其冲地遭到计算机攻击，包括银行与金融业、通信或其他公用事业部门。计算机系统的所有者和操作者是保卫其系统和信息的完整性、可用性和保密性以及数据的第一道防线。

对一次成功的攻击来说，只要对大多数美国人造成系统瘫痪就行了，而不一定去直接威胁生命。这样的攻击也不一定是在全国范围内发生。破坏一个大城市的电力供应，或停止一家全国性大银行的运行，其带来的剧烈震荡远远超过了直接受害人数。

我们的基本认识是：对联网的信息系统及其所支持的基础设施的威胁就在于它们过于脆弱，而且敌手有能力和兴趣发动攻击。对付这种无所不在的威胁的唯一办法就是认真评估并



纠正脆弱性，同时准备快速反应和重建的工具。如果不采取这些措施，我们将会因失察于即将到来的威胁遭到失败，这是一种可以把美国商业、社会和政府置于危险境地的失败。

## 2. 保护隐私与公民自由

这篇国家计划中的提议将会加强公民的自由与隐私权。人们早就认为，某些计算机安全工具可能会给言论自由迎头泼上冷水。还有些人认为，如果限制公民的匿名通信，或者收集和分析与网络使用相关的数据，则政府和私营部门会侵犯到网络用户的隐私。

关键基础设施保护总统委员会（PCCIP）是应行政令 13010 创建的。自从该行政令发布以来，管理部门已经分析了在维护和加强美国公民隐私权的情况下对关键基础设施保障对象提供支持的过程和组织结构。在 PDD63 中，总统强调了隐私权的重要性。

正如本章所描述的，政府将把公民自由与隐私权作为基础设施保护综合性国家战略的一部分。仅仅关注公民特权而不在一个特定的过程中研究各种相关复杂问题是不够的。本章讨论信息保障与隐私保护之间的关键问题与潜在冲突，还介绍了这篇国家计划对该类问题的解决途径。

### 可提高隐私保护的关键基础设施项目

在实现基础设施保障目标的同时还必须维护甚至加强美国公民的隐私与自由权。一些基础设施保障项目可以通过提高网络环境中数据与通信的安全级别来增强个人隐私权及其他公民自由权。虽然基础设施保护将导致雇主，包括政府和私营业主保留一定的网络监控权利，但如果与现行法律和保护条例保持一致的话，这将会与公民自由发生矛盾。既然这些监控是发生在雇主拥有的网络上，并且是专门用来发现网络滥用的，那么这些项目既保护了公司和用户，也没有对隐私保护权造成无理侵犯。

国家计划中包括了一系列能够保护个人隐私的项目，包括：

- 要求政府“成为领导范例”并“促进安全意识”，在政府内支持对隐私和通信可靠性给予更多的关注和强调，从而设置强制性标准以供私营部门遵循。
- 开展教育和培训，包括对计算机伦理学的强调，促进大家对通信隐私的尊重。
- 施行脆弱性评估，为保护政府和私营部门的关键性资产而投入资金，确保这些网络上的通信保密。
- 在政府和私营部门之间建立伙伴关系，促进在信息安全目标下的自愿合作。
- 作为关键基础设施保护计划的一个重要部分，对公民信息加以保护；加强对公民个人保密性信息的安全保障。
- 使所有的基础设施保障项目与现有法律保持一致，如《电子通信隐私法》（ECPA）、《隐私法》以及其他相关法律。
- 必要的时候，对监控进行认真规划，使其限制在取得预定的基础设施保障目标活动和目的范围之内。

联邦政府认识到，如果不慎重使用为信息和系统保护所设计的技术，公民自由就会受到不可避免的伤害。即使出于最善意的目的，如果技术使用的范围太广，那些清白的活动也有可能处于监视之下。在涉及个人权利时，慎重考虑所有相关问题是很有必要的。

法律并不总能在权限、安全标准、许可协定等方面提供清楚的指导方针。计算机入侵常常造成复杂的法律和司法问题。因此，保护基础设施和公民自由的政府项目要求进行仔细的计划和分折，并需要考虑到所有的参与方。

这篇国家计划中的提议保持了与现行隐私法和期望的完全一致。计划号召每年召开一次有关计算机安全、公民自由和公民权利的公共-私营界讨论会，以确保计划的实施中时刻考虑到公民自由，并确保与政府内外计算机安全专家的提议和公民的权利考虑保持一致。

国家基础设施保障委员会（NIAC）由来自联邦政府之外的参与者组成，它也将每年对计划执行中有关公民自由、隐私权、私有数据保护的活劫进行审查。

### 国家计划的目的

在这个复杂的环境中，有必要理解本计划的历史以及政府在实施各类项目时的意图。以下三个方面尤其值得注意。

第一，本计划是多方参与和努力的结果。早在 1995 年，当政府对几个可能的基础设施保障战略进行评审时，多方合作就被认为是一个好方法。PCCIP 报告中的总结和建议（已并入 PDD63 和本计划中）中包含了很多来自于学术界、工业界和很多政府机构团体的富有价值的看法和见识。政府已经把这些年来获得的知识融入到这篇计划中的项目和实施战略中。

第二，本计划的启动和初期阶段主要依靠现有的法律、制度及项目，因此计划中融入了这些法规和条例中的保护事项。这种理念与已有的机制协调、利用并合作，是基于这样一种认识：基础设施的保障是不会一蹴而就的。其他的一些相关理念包括：

- 依靠自愿性合作来实施计划；
- 与私营部门，包括所有者和运营者合作，而不是施加新的联邦法规。
- 关注并促进私营部门和政府间的合作联盟，这样各方均能够明晰并认可其私有利益将遭到的冲击。

第三，也是最重要的，这个计划不会以牺牲公民自由为代价来换取基础设施的保障。国家计划的实施将严格遵守现有的传统和制度，也不会违背宪法和联邦法律所规定的安全措施。在计划的实施过程中，联邦政府必须遵守所有保护公民自由和隐私权的现行法律，并且不会为了实现其基础设施保护目标而制定侵犯性的政府条例。

### 关注

计划中列举的一些项目可能会引起对公民自由的关注。但是由于计划的很多其他部分对公民自由保护机制和实施战略只字不提，也许会使读者错误地得出如下结论：基础设施保障目标的实现可能会以个人隐私权的牺牲来换取。但事实并非如此。

在计划中最重要的一部分是联邦入侵检测网络（FIDNet）。FIDNet 是一个入侵检测感应器网络，用以保护民事联邦机构中的关键系统。这些感应器以多种方式来搜寻攻击者并发布警报。

FIDNet 的几个重要特点，包括：

- 对关键系统节点上的入侵进行检测；
- 是一个事件报告和处理的自动系统；
- 位于总务管理局（GSA）的中央管理式的运行结构用于对受感染的关键基础设施系统的状态进行处理、发布、报警以及协调。

重要的是，FIDNet 的构架非常精细，可以确认出很小的入侵类型。FIDNet 着重关注对联邦所有非公众网络系统或领域发动的攻击。FIDNet 要求任何政府机构参与方在与现有法律保持一致的前提下持续监控其各自的网络。司法部所做的一次法律上的预审早已得出结论：在一定限制下，FIDNet 的概念遵循了《电子通信隐私法》（ECPA）。然而，随着 FIDNet 概念不断发展，一个跨机构的法律审查小组将继续检查 FIDNet 对 ECPA 以及很多其他法规，如 1974 年的《隐私法》的遵循问题。

### 解决方案

在基础设施保障中对公民自由的保护是一个动态过程，这个过程既涉及了政府，也涉及了私营部门。在这一过程中，我们必须认识到现有司法制度的复杂性和重要性，并要建立新的项目来预防意外结果的出现。

在这样的大势之下，作为分析这些项目的起始点，有 9 个关键准则要遵循。

- 与隐私权团体协商以定义解决方案：联邦政府应该要求隐私权团体加入解决方案的起草，以支持国家计划和公民自由权。要关注 3 种复杂性，即（1）公民隐私法和政策；（2）国家计划中的项目；（3）支持这些项目的技术问题。隐私支持者要确定其可能的关注范围并制定出合适且合法的解决方案。
- 对国家计划中各项目的严格而彻底的法律审查：一个跨部门的法律评审小组将检查这一国家计划的初期活动，以确保有关隐私与公民自由权的事项在计划中得到了考虑。
- 遵循现有的立法机构所制定的保护法案：国家计划中的项目必须满足国会认真制定的标准。各种法规，包括《电子通信隐私法》、1974 年《隐私法》以及 1987 年《计算机安全法》，要对国家计划的相关活动做出管理和约束。这篇国家计划认识到各种公民自由法案的复杂性，尤其是国会和司法部所扮演的重要角色。
- 领导榜样：在信息安全和相关的基础设施保护领域中，政府仍将成为领导榜样。这包括更优、更完备的信息安全培训和教育以及对政府手中信息的保护。例如，在政府的新型计算机系统开发的标准步骤中将加入对安全和隐私的评审。
- 对各种各样的隐私解决方案的评审：关键基础设施共同体要参与对隐私解决方案和操作的彻底评审。具有隐私问题实践技能和专业知识的政府机构，包括 OMB（管理和预算办公室）和联邦贸易委员会，将继续协助相关隐私政策的开发。
- 与国会合作：国会负责隐私和公民自由的立法事项。作为评审过程的一部分，国家计划起草者将会向国会咨询，包括具有专业技术的国会机构，如国家审计总署等。
- 与国家科学院合作：政府所面临的挑战之一就是要开发保护基础设施和公民自由所需的技术。而国家科学院和国家工程院在这些领域具有丰富的经验。它们中的很多组织，如计算机科学技术学部已经对医疗信息的保护和其他技术做了研究。
- 关注教育和培训：国家计划的任務包括对公众加强公民自由和隐私问题的教育。教育和意识培养项目将关注计算机伦理学和其他相关主题。
- 遵守隐私原则：国家计划将遵守由信息基础设施任务组隐私工作组制定的《个人信息提供和使用原则》。这些原则涉及信息隐私、信息完整性、信息质量、信息获取、信息提供、个人信息保护以及信息使用公平性等事项。

遵循这 9 个原则将有助于促进对国家计划的目标和美国隐私保护的清晰理解，确保个人自由这一信条能融入到国家计划的项目中去。

### 3. 计划的目标和范围

#### 计划的目标

由敌对势力或恐怖组织发动的有组织、有计划的计算机攻击使我们国家各个组成部分所面临的威胁不断增加。对商业来说，这种威胁使其生存能力、公众信誉、顾客关系及投资者信心都受到损害；对政府来说，它使关键服务无法可靠地向国民提供；对国家安全来说，它使军事、情报和外交反应被打乱或受到损害。

我们的这篇国家计划概括了为使这些威胁降低到能被美国人民所接受的级别而需采取的步骤。

在 PDD63 中，总统确立了一个国家目标，即美国应该获得并保持“保护我们国家的关键基础设施的能力，以防止可能会严重危害到下述职能的有预谋行为：

- 私营部门确保经济有序运行以及重要电信、能源、金融和运输服务的正常提供。
- 州及地方政府维持有序运行，提供最起码的重要公共服务。
- 联邦政府执行其重要的国家安全责任并确保公众的健康和安全。

这些关键功能遭到的任何破坏或操纵都必须控制在跨时短、频率低、可控、地域上可隔离以及对美国的利益损害最小这样的规模上。”

#### 国家计划的范围：关键计算机和信息系统的安全性

20 世纪 90 年代在美国发生的信息技术革命以及国家和社会对信息技术革命所产生的信息系统的依赖，使国家级别的信息系统安全和防御项目变得极为重要。任何国家信息系统安全和防御计划都必须覆盖一个广阔的范围。

作为国家计划的第 1 版，本文的重心在于关键信息基础设施系统对计算机和物理攻击的保护。对其他关键物理基础设施及其安全的考虑正由另外的工作组开展。

关键性物理基础设施的安全是 1995 年评审的重点，该次评审由 PDD39 指示并由司法部长负责。关键性物理基础设施多年来一直是 FBI 重要资产行动（KAI）和国防部重要资产保护项目（KAPP）（现在包括在国防部关键基础设施保护项目之内）的重点。因此在关联文档中，我们可以找到很多讨论大坝、桥梁、隧道、输电线、电站等设施安全性的计划和项目，并可以看到它们同很多其他关键性信息基础设施系统的互依赖性联系。

这些已有的关键性物理基础设施安全项目也要受到新的评审，而且在 2000 年会发布《国家关键性物理基础设施保护计划》。两个计划（加上《信息系统及关键性物理基础设施保护计划》）将就所确定的横向事项进行协作并最终融合成一个计划。

正如 PDD63 所号召的，处于领导地位的各联邦机构正在与每一主要经济领域（如运输业和银行业）内的公司合作开发关键基础设施保护计划。每个联邦部门都应开发保护其各自关键基础设施，包括计算机和物理层面的计划。联邦各部应与对应的私营部门在适当的方面开展合作，开发它们自己的信息系统和关键性物理基础设施保护计划。

下表显示了这篇国家计划是如何完成其联邦计算机安全和信息资源管理（IRM）责任的：

国家计划实施	IRM/管理责任
确认联邦政府内的主要节点和各关键基础设施系统依赖性	OMB: 应 OMB A-130 的要求, 使用这些信息来管理各机构的脆弱性并进行风险评估
确定主要的国家安全资产和基础设施系统	OMB: 应 PDD63 所要求, 使用这些信息把基础设施保护工作并入《政府工作表现和结果法》(GPRA) 机构报告中
确定基础设施系统需求、依赖性以及共有的危险和脆弱性	各机构的 CIO/CFO: 使用这些信息使预算提议关注于关键基础设施系统
确认基础设施系统威胁、脆弱性; 确认联邦系统的哪些地方存在公有的危险和脆弱性	各联邦机构: 应 A-130 要求, 使用这些信息评估各机构关键性信息系统的脆弱性和风险; OSTP 和 OMB: 使用这些信息来使研究和开发议程得到集中
确认并寻求与私营部门伙伴的合作; 确认基础设施依赖性以及共有的威胁和脆弱性	CIO 委员会: 使用这些信息来制定私营部门推广计划; 充分利用在这篇国家计划的结构下建立的各类关系

### 联邦计算机安全和 IRM（信息资源管理）责任

管理和预算办公室（OMB）承担了联邦计算机安全和信息技术管理的核心责任，与我们的国家计划关注于国家安全系统并强调与私营企业合作所不同的是，OMB 对联邦自动化信息系统安全政策的制定有着法定的责任。它制定的一些主要政策见下表：

焦 点	法 令
计算机安全和隐私——确保公众对数据的访问	1987 年计算机安全法
绩效表现和结果——管理各机构的职能表现	1993 年政府绩效和结果法
效率——最大程度地利用收集到的信息，尽量减小公众对数据请求的负担	1995 年减少文书工作法
机构管理 IT 的责任——采购、投资、安全。在每一机构中都建立 CIO 职位	1996 年 Clinger-Cohen 法
OMB 通过 CIO 委员会的建议和监督来实施其核心原则	行政令 13011

OMB 实现这些要求时主要依靠 OMB A-130 通告的附录 III “联邦自动化信息资源的安全”。通告中要求 OMB 监督运行规范和标准的开发以及对脆弱性和风险的评估，还要负责管理公众对信息的访问。OMB A-130 对上述每一事项都有详尽的说明。在过去的几年中，OMB 还发布了很多其他的相关资料，涉及如下内容：

- Internet 和网站隐私声明；
- 推荐的计算机操作规范和标准；
- 大型系统的采购。

### 联邦预算

自从总统于 1998 年发布了 PDD63，用于保护关键基础设施的联邦拨款一直在增加。在 2000 财政年度制定的预算中将有 17.37 亿美元用于关键基础设施保护。这比 1998 财政年度的预算（该年度财政预算的制定正好早于 PDD63 的签署）增加了 50%（见附录 B）。

在为 2001 年财政预算请求所做的准备中,OMB 与国家协调员合作建立了一套特殊步骤,在国家各部和机构提交其预算之前评审国家和各部在安全领域内的要求(见附录 B)。

这一新的评审步骤旨在确保以下事项:

- 各机构和部门在拨给他们的总款项中拨出足够的资金来实现 PDD63 中的总统意图、OMB A-130 中的指令和《计算机安全法》的要求。
- 在以后的总统预算中要在国家级别上提出要求,还要提出与每一具体的联邦部局有关的明确要求。
- 总统对 2001 年预算草案进行评审,确定与该篇《信息系统保护国家计划》有关的决策点。

我们的这篇国家计划得到了总统的支持,为联邦各部和机构准备其预算提供了广阔的方向和指导方针,但它并不是一个决定预算的文件。各机构对于信息系统保护的拨款将由常规的 OMB 预算制定过程做出决定。

因此,该版国家计划中的时间表只是方向性的。精确的工作任务、资源消耗以及完成日期将在国家计划的后续版本中有所调整,并将把总统和国会所做的特殊预算决策考虑进去。

### **建立公共-私营合作联盟**

建立公共-私营合作联盟是这篇国家计划的一个核心主题。没有私营部门的完全参与,联邦为保护关键基础设施所做的努力将会收效甚微。

在该版计划中,私营部门和州及地方政府保护关键基础设施框架仅是一个初步的纲要,联邦政府还要继续建立必要的合作联盟。当这些合作联盟都确立起来后,我们希望这个计划也能反映出私营公司和组织的想法和决定,而不仅仅是联邦政府的。

为了建立公共-私营合作联盟,联邦政府要求负责运营关键基础设施的全美所有的商业领导人加入该计划,并且要使他们意识到加强计算机的安全性的需求。1999 年 12 月,超过 85 个公司的高级执行官在纽约讨论了建立关键基础设施合作联盟的计划。下一次会议在 2000 年年初召开(见执行摘要的内容 8 或第 4 章)。

### **与国会合作**

行政部门将同国会继续密切合作以开发必需的关键基础设施安全保障工具和措施。这些措施中不仅包括拨款,还包括解决很多法律和政策问题的建议和帮助。国家计划的后续版本中必须建立同国会的真正对话途径,就如何更好地保护我们的关键基础设施以实现其安全性和蓬勃发展同国会进行良好对话。

行政部门和国会已经开始了这种对话和合作,并在该版国家计划中获得了一些成果。随着国家计划的不断成熟,还会取得更大的成绩。国会议员已经引入了一些立法提议,举行了听证会来讨论有关问题,并为法律改革奠定了坚实的基础,以满足基础设施保护所提出的要求。这些议员提出了很多棘手问题,涉及个人隐私权保护以及联邦政府在监控基础设施遭到的计算机攻击活动中所担负的角色等。而且在听证会上,他们要求对方对这些问题做正面的回答。这篇计划曾经历了这些国会议员的很多类似锤炼。

持续而充足的资金对计划的有效实施以及初步功能的建设是很重要的。但我们也还需要法律上的援助,以确保政府能够同私营部门建立稳固的关系,排除这类合作的法律障碍并提供增强性的法规和框架。为取得这些目标,行政部门将向国会寻求建议及帮助。

## 两个组成计划

在我们促进国家重要计算机系统安全性的工作中，《联邦政府关键基础设施保障计划》和《私营部门及州和地方政府关键基础设施保障框架》，即国家计划的两个组成部分是我们工作的核心。正如这篇国家计划所示，政府民事机构的工作正处于初始设计阶段。国防部的工作已取得了长足进步并已经开始实施。作为合作伙伴的私营部门集团（国家计划曾为此做出了建议）却仍处在襁褓阶段。国家计划的后续版本将融和美国关键基础设施各个领域，包括银行与金融、紧急事件服务、能源、电信和运输内的计划。

## 未来战略

这个多年度的计划包括了那些我们认为对于保护关键基础设施所必需的主要活动。它为我们国家的各个部门——私营部门、联邦政府、州及地方政府提供了明确的方向，并且代表了我们在新千年为保护关键基础设施所做的承诺。

## 4. 联邦政府关键基础设施保护计划

总统已经号召联邦政府成为信息系统安全的典范，但如今，情况并非如此。

政府越来越依靠计算机和网络来组成其关键的信息基础设施，为我们的社会负担诸多非常重要的功能——从我们国家范围内公民权利的保障到对重要服务连续性的依赖。最近，几起针对政府计算机网络的非法入侵已经使政府加强了提高其防御能力的决心，以抵御计算机犯罪、计算机恐怖主义以及信息战等可能直接威胁到联邦政府基础设施的事件。

这篇国家计划的联邦政府部分展示了由政府计划并正在执行的对这些基础设施系统提供保护的一些行动。政府各部和机构正纷纷准备他们自己的计划以保护其关键基础设施，同时也已有了新的处理步骤来确保各机构之间的协调以及这些计划的一致性。横跨各机构的活动也已发起。事实上，开发一个联邦范围的计划可以把政府内的各机构前所未有地紧密联系在一起，而以前这种合作是不多见的。协调的过程之所以必要是因为我们的政府所依赖的计算机网络和系统之间具有多边联系以及互依赖性。

联邦计划分两节说明，在其前面还包括一个对保护关键信息基础设施的有关联邦组织的描述。两节的内容概括如下。

- 民事机构保护及政府级行为：这部分计划讨论联邦民事机构的基础设施保护方案，包括法律的使用。它概述了在联邦政府的范围内现行的有关活动，还给出了某几个联邦机构借以确定对它们最为重要的信息基础设施的活动的例子。该部分还包括：评估和确定潜在的弱点；提高相关能力，以标识和预防任何针对关键系统的有意攻击并减缓其带来的危害。
- 国防部基础设施保护计划：由于其保家卫国的任务性质，国防部成为第一个响应该篇国家计划的政府部门。在所有国家部门之中，国防部的计划及随后的执行也是最成熟的。并且，在很多重要方面，它成为其他部门、机构的范例。于是，反映国防部独一无二的作用领域和任务的材料以及那些可以作为其他联邦政府部门范例的活动在这节中均做了详细的说明。

### A. 负责关键基础设施保护的联邦组织

1998年5月22日，总统发布了第63号总统令（PDD63），号召举国努力来保障脆弱性日益增加的美国互联基础设施的安全，尤其是基于计算机的基础设施的安全。这些基础设施

包括电信、银行与金融、运输业、供水系统以及重要的政府服务。总统令要求联邦政府立刻评估其基于计算机的那些系统的脆弱性并矫正缺陷，而且，还要求制定详细的计划来保护关键基础设施并对国家进行防御以对抗信息战。总统令命令，政府应当在国家中成为保护基础设施的楷模，公共部门和私营部门要联合起来保护关键基础设施。

PDD63 组织了如下联邦政府组织和人事来迎接日益增长的安全挑战。

- **安全、关键基础设施及反恐怖主义国家协调员**在白宫国家安全委员会（NSC）监督关于关键基础设施保护的国家政策的制定以及执行。国家协调员是内阁首脑委员会的一员，向总统和国家安全顾问提出关于国家关键基础设施政策和执行方面的建议。NSC 关键基础设施高级负责人对其提供支持。
- **关键基础设施保障办公室（CIAO）**是一个跨机构的办公室，位于商务部，旨在支持政府机构和私营部门的计划制定。办公室还负责评估各机构对关键基础设施的依赖度，协调国家的教育和意识培养项目、法律问题以及公共事务。
- **国家基础设施保护中心（NIPC）**是一个位于 FBI 的跨机构办公室，职能是作为威胁评估中心，关注威胁报警、脆弱性以及执法问题。NIPC 包括由 FBI、国防部、美国特工处、各情报机构以及其他政府机构派出的代表。
- 对每个可能成为计算机或物理重点攻击目标的基础设施部门来说，都有一个专门的国家部级机构作为联络时的领导机构。该机构还将指派一个部门联络官在基础设施部门中指导事务。PDD63 中规定的基础设施部门及相对应的领导机构如下表所列：

关键基础设施部门	领导机构
信息与通信	商务部
银行与金融	财政部
供水	环境保护局
航空、高速公路、货运、输油管道、铁路、水路贸易	交通部
紧急事件执法服务	司法部/FBI
应急消防等政府服务	联邦应急管理局
公共健康服务	健康和公众服务部
电子电力、石油和天然气生产和储存	能源部
联邦政府	总务管理局

- 部门联络官将与**关键基础设施协调组（CICG）**的国家协调员密切合作，CICG 是一个跨机构的委员会，职责是分析关键基础设施政策问题以及向内阁长官委员会提交政策建议。
- 那些没有私营部门参与的职能领域（国防、情报、国外事务、执法以及研发）在 CICG 由专门职能协调中心代理，具体见下表：

国务院	国外事务
国防部	国防
中央情报局	外国情报
司法部/FBI	执法和国内安全
科技政策办公室	研究和开发



## B. 民事机构保护和政府级行动

在本节所展示的政府行动中，联邦政府为私营部门关于如何最有效地保护关键信息系统基础设施树立了榜样。很多领域中的重要工作目前正在开展。

- **国家基础设施保护中心（NIPC）**继续履行其作为跨机构的国家关键基础设施威胁评估、警告、脆弱性分析以及执法调查和响应实体的职能。
- **专家评审组（ERT）**同联邦机构合作以改善信息安全状况，同其他负责信息安全事务的有关联邦实体协调工作。
- 作为历史上的第一次，联邦政府正在协调联邦机构对基础设施保护的研发（R&D）活动，确保各类计划、项目以及议程的一致性，把联邦政府的研发资源用在最重要的基础设施脆弱性研究上。

其他所提议的活动将有助于确保联邦政府的榜样地位。

- 建立全国范围内的攻击响应、攻击后重建和恢复系统。
- 向民事机构提供：关键的系统节点处的入侵检测系统；自动事件报告和处理系统；以及一个中央管理的运行结构，用于处理、分发、报警及协调功能，从而提供基础设施的计算机状态的连贯性报告。一个指导委员会正在调查操作上的诸类问题并决定联邦入侵检测网络（FIDNet）的技术体系结构。
- 建立关键基础设施保护国家学会来帮助开发和传播我们的信息基础设施保护所必需的相关知识，加速各种操作建议、标准、评估准则的开发，使其早日被联邦政府和私营部门所采纳。
- 通过联邦计算机服务（FCS）项目，解决受过系统安全和管理培训的联邦雇员严重短缺的问题，该项目将对更多的美国人施以信息系统安全方面的教育。
- 强化大学中的信息安全课程，建立 INFOSECURITY 优秀中心来保障本科生和研究生教育项目的发展，以适应培养高素质研究人员和信息系统安全专家的需求。
- 开展全民安全意识普及运动，提高对加强计算机安全的需求的理解与认识，第一批对象是所有的关键基础设施机构的业务领导、联邦雇员以及我们国家的在校学生。在此基础上，把受教育的对象逐步扩展到其他私营部门和普通大众。
- 对现有的法律提出必要的修改建议，以适应国家信息系统安全所面对的新威胁，这些对法律的改动要能确保国家关键基础设施的安全，同时确保公民的自由权。
- 与私营工业合作，通过公共-私营合作关系确保联邦政府的那些将对工业活动（或相关活动）产生直接影响的行动中能有工业界的适当参与。

**内容 1：标识关键基础设施资产以及互依赖性，查找其脆弱性**

### 1.1 联邦民事机构及其评估

联邦政府已经建立了很多组织结构，制定了相关计划，来保护其免于受到计算机攻击。

#### 1.1.1 政府各部的计划和信息基础设施保护的责任

- **部级机构关键基础设施保护计划：PDD63** 要求政府各部局制定保护它们的关键基础设施的计划。在 1998 年 11 月，拥有最重要系统的那些部门被指定为一级机构（Phase

One Agencies)，制定了它们保护其关键信息系统的最初计划。二期机构的计划在 1999 年 2 月制定。所有的计划都要在两年之内完成。

国防部对基础设施的保护可见第 C 节的描述。

如下期机构在 1998 年 11 月制定了它们的计划：中央情报局（CIA）、商务部（DOC）、国防部（DoD）、能源部（DOE）、健康和公众服务部（HHS）、司法部（DOJ）、联邦调查局（FBI）、交通部（DOT）、财政部、国务院（DOS）、退伍军人事务部（DVA）、环境保护局（EPA）、联邦应急管理局（FEMA）、国家安全局（NSA）。

如下二期机构在 1999 年 2 月制定了它们的计划：农业部（USDA）、教育部、住房和城市发展部（HUD）、内务部（DOI）、劳工部（DOL）、总务管理局（GSA）、国家宇航管理局（NASA）、原子能管制委员会（NRC）。

- 对于关键信息系统基础设施的物理性保护的特别关注：所有机构均有责任确定其信息系统的物理脆弱性并采取矫正性措施。关键基础设施的领导机关将同私营部门协同工作以矫正非联邦系统中的脆弱性。
- 持续发展中的专家评审步骤：关键基础设施协调组（CICG）建立了一个专家评审组（ERT）来帮助各部和机构改善不符合 PDD63 要求的地方。过渡期的 ERT 位于关键基础设施保障办公室（CIAO），并和联邦 CIO 委员会、GSA 和 OMB 合作。过渡期的 ERT 是联邦政府内的新机构。从此，我们第一次有了一个规模虽小但全职的工作组来投入到加强关键基础设施保护的工作中来，它的工作包括：
  - 提供 IT 安全方面的信息纲要；
  - 确保所有机构的计划框架的一致性；
  - 随时对 22 个一期和二期机构进行审查和评价。

在商务部的国家标准与技术研究院（NIST）内将建立一个永久性的专家评审组，负责帮助政府范围内的机构达到联邦计算机安全要求的标准。

- 首席基础设施保障官——评估并矫正脆弱性：依据 PDD63，联邦政府各部和机构均已指定了首席基础设施保障官，但对其是否与首席信息官（CIO）是同一个人没有要求。首席信息官负责信息保障，首席基础设施保障官则负责部级基础设施其他方面的保护。在每个机构所做的计划以及其执行过程中，关键的一项就是自我脆弱性评估。任何部或机构要向国家协调员确认其职能运行所依赖的关键系统。
- 核实过程：CIO 委员会将推动相关的审计过程，来核实各机构是否遵循了它们的基础设施保护计划。该过程的发展将在与很多组织，如 NSA、信息技术资源委员会、GAO 和 IG 的协调下完成。

### 1.1.2 进行脆弱性分析以独立地测试安全性

- 各机构将开展一些项目来完成某些种类的脆弱性测试和分析，包括：利用 COTS（商业现货）工具、常规 Internet 自我评估工具、独立的外部关键性评审等方式进行日常自动化系统配置/完整性/脆弱性测试。

应各机构的要求，NSA 和 NIST 将开展一次独立的联邦关键信息基础设施分析，独立的结果报告将交给各个机构的 CIO。所有联邦机构都要指派自己的代表，该代表可以向对其计算机系统的访问进行授权，以推动脆弱性和模拟攻击分析。司法部将建立法律指导方针来促进对美国政府实体的脆弱性评估的顺利开展。另外，在独立评估中，各机构的总检查长应当

担任重要的角色。CIO 委员会和国家协调员将和各机构的总检查长合作，促进他们对这些问题的注意。

### 部级关键基础设施保护计划的专家评审

新生的和创新性的概念

专家评审组（ERT）建立于 1998 年 11 月，在确保各机构所制定计划的质量、一致性和执行有效性以保护其关键基础设施的道路上，这是一个里程碑。它是第一个具有如下功能的跨机构小组：

- 在 CIP 计划制定过程中引入了连贯性、政府级经验以及综述。
- 要求各机构的信息安全计划遵循跨机构间达成的关于在计划中要包含公共基本计划要素的规定，并对此做出**审查和评论**。
- 对计划的执行提供始终如一的监督和支持。
- 使联邦机构更容易得到技术协助。

第一阶段

在其工作的第一阶段，ERT 关注各机构计划对公共要素的纳入情况，并对初期计划中这些要素的纳入情况做出评审。这些要素是：

- 该机构的任务以及对其职能运行时所依靠的关键性基础设施的确定；
- 威胁分析；
- 脆弱性评估；
- 矫正计划；
- 应急计划；
- 研发要求；
- 角色和责任；
- 资源要求；
- 执行日程表；
- 协调工作；
- 人员招募、留任、教育以及意识培养；
- 法令以及指导方针。

在该阶段，ERT 有可能：

- 发现机构在最初的计划准备过程中经历了研发、资源、要求、协调等方面的巨大困难；
- 鼓励机构在其计划中纳入所有的必要要素，以使计划的构架完整，可以在一个动态的基础上提供发展中的评估；
- 在必要的时候要求机构修改或重写计划；
- 采取在政府范围内和单独面向机构两种方式简单通报对初期计划的评估结果；
- 建立一个新的、互相协商后的处理方法，这并不是对机构计划的批判，而是协助其对计划做出改善；
- 达到了与机构的高度合作。

**第二阶段**

从评审计划到支持计划实施，ERT 的主要工作过程包括：

- 同一期和二期机构合作，也可以选择其他政府机构，协助它们确定与其职责相关的国家安全、关键性国家经济安全、关键性公众健康和安全责任的内容；
- 同一期和二期机构合作，也可以选择其他政府机构，协助它们确定在履行各自负责的国家安全、关键性国家经济安全、关键性公众健康和其他与安全相关的职责时的基础设施依赖性以及同 IT 有关的互依赖性。

**联邦各部加强计算机安全的行动时间表：**所有的联邦机构都应该确保其职能运行所依赖的、符合信息安全保障标准的那些关键计算机和信息系统能得到安全保护。对这些系统，各部局应该执行脆弱性测试，确定互依赖性、制定事后矫正和恢复计划，并定期更新计算机安全措施。具体见下表：

阶 段	行 动	目 标 日 期
1.1	联邦一期机构完成最初脆弱性评估，制定矫正计划。ERT 将分析其报告	已完成（1999 年 2 月）
1.2	联邦二期机构完成最初脆弱性评估，制定矫正计划。ERT 将分析其报告	已完成（1999 年 5 月）
1.3	联邦各机构向 OMB 提交一份多年度的脆弱性矫正计划，同时提交 2001 年的预算，以后每年如此。ERT 将和各部合作执行其矫正计划	已完成（1999 年 6 月）
1.11	联邦政府制定用来标识关键基础设施资产和互依赖性的方法	2000 年 9 月
1.14	私营部门信息共享和分析中心将为会员公司开发一套用于评估和矫正项目的推荐方针	2000 年
1.16	私营部门信息共享和分析中心将评估各私营部门和工业界公有的脆弱性	2000 年
1.17	国防部将建立合适的组织结构来标识和矫正脆弱性、开发并配置入侵检测系统、开展重要的创新研究和开发项目	2000 年 11 月
1.21	联邦机构应已经完成了信息系统脆弱性评估，采用了多年度资金计划来矫正这些脆弱性，创造了用于持续更新的系统。每一关键行业的私营部门公司也应做到这样	2000 年 12 月
1.29	矫正计划应已经消除了联邦机构和主要公司的关键信息系统绝大部分的已知脆弱性。脆弱性评估和矫正还要继续下去	2003 年 5 月

**信息系统物理安全保护时间表：**为了解决关键计算机和机控系统的物理安全问题，联邦政府将采取下表的行动。

阶 段	行 动	目 标 日 期
1.7	联邦政府完成关键物理基础设施保护计划的第 1 版	2000 年 6 月
1.12	国防部将完成其关键计算机系统物理保护的检验和评审，包括涉密和非涉密网络	2000 年 9 月
1.15	国防部将更新其对关键基础设施保护项目的检查，以针对同关键计算机网络相关的基础设施的主要脆弱性而确定并推荐矫正意见	2000 年

## 1.2 关键信息系统计算机安全的操作建议 and 标准

对美国政府的关键信息系统安全的保护是至关重要的，政府既是国家基础服务的提供者，也是国家其他领域参照的楷模。在政府的多重角色之间要达到和谐的平衡。一般来说，政府不会开发其自己的安全解决方案，但它可以向私营工业寻求标准和操作建议、COTS 产品以及咨询服务。然而，作为世界上最大的信息系统，联邦政府要在计算机安全产品、操作建议、标准的开发和使用过程中担任重要的角色。

除了各机构的计划外，OMB 和 GSA 将和其他机构合作完成如下活动，以确保美国政府在信息系统安全方面对其他国家的示范作用。

- 为关键联邦信息系统确定和采纳建议及安全标准：NSA 和 NIST 负责为涉密以及敏感但非涉密的联邦信息系统制定标准。OMB 和 GSA 在确保联邦信息系统安全方面扮演其他方面的重要角色。这些权威机构——NSA、NIST、GSA、OMB 和国家协调员合作，将为联邦关键信息系统确定和开发操作建议和标准。在同 CIO 委员会的协调下，各机构将确认他们的关键信息系统并在 2001 年以前执行这些操作建议和标准。

这些措施将依赖于对安全技术和操作建议进行采纳的能力。一个三步过程将用于开发联邦使用的操作建议和标准：

- 第一步，确认并利用现有的私营部门或联邦部门的标准和操作规程。
- 第二步，如果必要的话，同现有的私营标准化团体和专业协会合作，开发新的或改正现有的私营部门标准及操作建议，从而满足联邦信息安全的需要。
- 最后一步，也许需要开发联邦政府有特殊要求的自定义标准和操作建议。

我们希望并鼓励在政府和私营部门能够采纳或改编统一的信息系统安全推荐标准和操作建议。

- 建立采购标准：GSA、DoD（只负责自己的采购）和 OMB 将同 NIST 及 NSA 合作来修订采购规章，要求对信息安全产品、系统和服务的获取必须符合联邦关于信息系统安全的操作建议和标准。GSA 和 OMB 将为各机构采纳和执行规章确定出步骤和期限。通过 NIAP（国家信息保障联盟）以及通用准则（CC），NIST 和 NSA 已经制定了这些采购标准的框架。NIAP 正委托商业实验室根据信息技术安全国际通用准则对安全产品/系统开展安全性评估和有效性检验。政府的政策规定了必须呈阶段性并有步骤地采用经过验证和评估的安全产品/系统，这推进了政府和工业界的合作关系，为信息安全提供了产品/系统基础。
- 开发安全测试和评估步骤：NIAP 致力于 3 个主要的活动来促进 IT 安全保障产品和系统的开发及使用：安全要求、安全产品测试以及安全测试研发。
  - 安全要求活动是一套由 NIAP 提供的服务，旨在帮助感兴趣的团体制定稳健、耐用的安全要求，并且这些要求最终可以被授权实验室采纳来测试产品或系统的安全属性。
  - 安全产品测试活动极力展示和提高在信息技术领域独立测试和认证作为安全和信任的手段的价值；使现在的这种由政府实施的评估和检测行为交由授权的私营部门实验室去完成；帮助建立起稳固的商业安全测试工业的要素；建立安全产品评估结果的国际双向认可的基础。
  - 研发活动的目标是通过 NIAP 资助的工业界合作以及研发界自身的努力，使关于安全测试方法和准则的研发称为一门尖端技术。
- 加强对联邦机构的监督，使其对系统漏洞和脆弱性做到实时维护，这种监督和要求对其他的系统安全保障活动也同样适用：FedCIRC（联邦计算机事件响应功能中心）是 NIPC 的一个计算机公告项目，它和其他 CERT 均可以实时提供关于最新的系统脆弱性和入侵模式的通告。应立刻对这些信息做出反应，否则它们将会失去其巨大

价值。GSA 将同 OMB 合作规定一套步骤来确保所有的机构都对 FedCIRC 和其他 CERT 的建议做到及时的采纳。该套步骤可能以 DoD 的（信息保障脆弱性预警）项目为模型。

- 制定用来确定联邦系统管理员及其他主要信息系统官员的步骤：有一些联邦安全相关工作职位是要有正式的认证才能担任的。NIST 和 OPM 已经为《计算机安全法》的实施准备了一个培训要求指南，该指南对很多相关的安全职位做了认定。

OPM 以及商务部和国防部将确定那些要求得到认证的联邦工作职位，还要规定一整套步骤用于证明一个官员是否具有熟练技能以胜任对其系统上的信息安全保障及维护，同时对于系统遭到的攻击能给予充分的响应。在规定这套步骤的过程中，将仔细考查现有的专业认证方案对联邦人事制度的适用性。

- 为联邦信息系统操作建议和标准制定正式的跨机构年度修订步骤：就像每年都要起草年度预算报告一样，对于联邦信息系统安全操作建议和标准的修订也应有一个年度的评估和考虑。OMB 和 CIO 委员会将管理这一跨机构的活动的执行。欢迎工业界和外界的标准化组织以及计算机安全组织参与这一活动。

**计算机安全操作建议及标准制定时间表：**要为计算机安全制定或开发操作建议和标准；使联邦政府内的关键性职能依赖系统，包括对系统的采购能够采纳这些建议和标准；制定职责明确的管理系统以达到这些标准的要求。时常对标准和操作建议做出更新；和工业界合作，鼓励它们采纳或改编这些由联邦政府推荐的操作建议和标准以供私营部门使用，鼓励国际标准化团体采纳或改编这些标准。

具体见下表：

阶 段	活 动	目标时间
1.4	CIO 委员会将成立关于联邦信息系统安全操作建议的一个跨机构工作组，它主要致力于确定、协调以及巩固正在开展中的政府安全操作建议制定活动。工作组将至少每年向 CIO 委员会做出安全操作建议的推荐报告。工作组还可以向 NIST 修订的联邦信息处理标准提出建议。NSA 和 NIST 将依据 1987 年的《计算机安全法》继续制定操作建议	已完成 (1999 年 11 月)
1.5	联邦政府将开发一个试验性框架及数据库，还包含若干实例，以确定并记录下那些能够确保关键信息资产安全的操作	已完成 (2000 年 1 月)
1.8	关于操作建议的跨机构工作组将至少每年一次向 CIO 委员会提出有所推荐的新的或修改过的操作建议的书面报告。CIO 委员会将会对每份报告都进行发布，同时附上评论	2000 年 6 月
1.13	联邦各机构将确保软件补丁的实时安装以及其他计算机系统脆弱性矫正措施的实施。必要时，OMB 将监督这一过程的执行情况	2000 年
1.23	不晚于 2001 年，联邦各机构应当在法律要求的范围内向 OMB 和 NIST 报告他们对相关的安全操作建议和联邦信息处理标准（FIPS）采纳的程度	2001 年 1 月

### 1.3 公钥基础设施：确保关键信息系统安全的公钥密码学

对联邦政府和私营部门的关键基础设施进行保护需要 PKI（公钥基础设施）的开发。通过以安全、可伸缩、可靠的方式分发公钥的公共密钥密码方法，PKI 确保了数据完整性、用户鉴定和认证、不可否认性以及数据保密性。PKI 的潜力使联邦政府和私营部门中间催生了

无数的计划和试验。联邦政府已经为 PKI 技术的发展做了积极推动，制定了集中各方力量来合作开发完整功能性 PKI 的策略。

PKI 系统通过公钥证书及产生相关的状态信息来分发密钥。状态信息一般作为证书注销表（CRL）来发放。产生证书和 CRL 的机构称为 CA（认证中心）。依靠管理证书和 CRL，PKI 支持数字签名和对称密钥的安全发放。

为了达到集成式的联邦 PKI 的目标，保护我们的关键基础设施，联邦政府正和工业界合作完成下列工作：

- 把各机构间的 PKI 互联入联邦 PKI 之中：DoD、NASA 以及其他政府机构正积极实施它们自己的 PKI 项目，以保护它们的内部关键基础设施。虽然这是很有意义的一步，但却无法保护各机构边界处的基础设施。完整的保护方案需要的是集成式的、全功能的 PKI。

为了促进各机构间 PKI 的互联，联邦 PKI 指导委员会（位于财政部）正开发一个联邦桥 CA。各机构只要和桥 CA 建立一条联系后就能与接入桥 CA 的其他机构 PKI 建立非直接互联。

为了推动各机构 PKI 所颁发的证书的兼容性，联邦 PKI 技术工作组已经开发了一个**联邦证书和 CRL 轮廓**作为政府机构的指导。遵循此指导的联邦机构的用户将能够处理彼此的证书。

- 连接联邦 PKI 和私营部门的 PKI：私营部门集团也正积极发展他们自己的 PKI。虽然这一步是很有意义的，但同联邦部门的情况一样，这些互相隔离的 PKI 不能保护跨越联邦政府和私营工业边界的基础设施。

把联邦 PKI 和私营部门 PKI 相连时会遇到联邦 PKI 互联同样的问题。联邦桥 CA 机制则将促进联邦 PKI 和私营部门 PKI 之间的互联。桥 CA 将对外部 PKI 进行分析，确立起各 PKI 之间的关系。此举使得联邦 PKI 的用户能够获得私营 PKI 用户的安全服务。

- 鼓励开发可互操作的 COTS PKI 产品：使用 PKI 的团体通常只限于采用一家提供商的解决方案。这无疑会极大地阻碍 PKI 的发展，因为大多数组织有着不同的计算机环境。因此，必须有可供用户选择的、适合其需要的 COTS PKI 组件，而不是采用特别提供商提供的组件。

《PKI 组件最小互操作性规范（MISPC）》规定了操作中的消息格式和传输协议以及上面提到的证书轮廓。对于详细消息格式和协议的定义将有助于可互操作的 COTS PKI 产品的开发。NIST 和一些 PKI 提供商如今正参与到一系列的互操作性工作组中，演示使用这些格式和协议的 PKI 组件的互操作性。

- 验证关键 PKI 组件的安全性：保护关键的基础设施需要对 CA 和相关组件进行合理操作。向关键基础设施所提供的安全服务的质量依赖于 PKI 组件的安全性。PKI 组件的安全性确保了关键基础设施所得到的充分保护。NIST 正制定一套用于 PKI 组件安全性的验证步骤。
- 鼓励开发能与 PKI 合作的产品：很多希望使用 PKI 的关键应用程序不一定支持和理解 PKI。为此，关键性应用程序需要选择 COTS PKI 来提供数字签名服务并管理证书。为了鼓励对支持 PKI 的应用程序的开发，政府正和提供商在主要应用程序领域展开合作。其中一个例子便是安全电子邮件项目已经在同工业界的联合努力中开始开发。

**PKI 开发时间表:** 建立把政府机构 PKI 和私营部门 PKI 连入全功能性 PKI 所必需的轮廓以及基础设施组件。发布互操作性规范以提高商业 PKI 产品的互操作性。建立验证过程以提高 PKI 组件的安全性。鼓励开发能与 PKI 合作的应用程序。具体见下表:

阶 段	活 动	目标日期
1.6	通过参照《PKI 组件最小互操作性规范 (MISPC) 》，使联邦 PKI 用户和外部 PKI 成员用户之间的证书和 CRL 轮廓得到增强，以满足 MISPCv2 的主要管理要求；建立联邦桥 CA，加强 PKI 组件的互操作性基准，满足 MISPCv2 的保密性要求	2000 年 2 月
1.22	展示能与 PKI 合作的应用程序的互操作性，比如，电子邮件，通过已出版的《证书发行及管理组件的安全要求》征求公众对 PKI 应用程序互操作性的意见	2000 年 12 月
1.26	首次检验 PKI 组件对《证书发行及管理组件的安全要求》的满足程度	2001 年 12 月

**内容 2：检测对政府计算机和数据进行攻击及非法入侵的多层系统**

美国的国家安全、经济利益、公众福利紧紧依赖于互联系统。对系统的恶意入侵却可以使这一互联网络陷入瘫痪、破坏或改变重要的公共纪录，甚至摧毁极端重要的公共服务，比如警务、消防、应急营救活动等。公众也希望他们发往联邦政府的数据能得到安全的保护，免于非法窥探和利用。但同时，公众也期望政府尊重和支持国人的隐私权和公民自由权。因此，任何联邦政府计算机和数据保护系统在设计时必须充分考虑上述诸类重要问题。

自从 1998 年第 63 号总统令发布以来，管理机关已经研究了大量同政府级计算机安全有关的技术、法律和政策。对政府计算机系统攻击的范围及频率都在增加，联邦机构正处在保卫其计算机系统完整性的巨大压力之下。更为棘手的是，我们还无法定量计算出由于系统攻击而导致的经济及日常生活的潜在损失——它们日益依赖于政府数据和相关的计算机系统。有关联邦信息系统的巨大依赖性的实例如下：

- 国防部及其他政府机构所负责的国家安全；
- 紧急事件报警系统所发出的预警；
- 国家气象服务中心发布的恶劣天气预报；
- 国家航空系统控制的飞行路线/空中运输。

很多公共和私营企业已经开始使用各种相关产品和服务来监督其计算机系统，防止计算机病毒和（或）网络非法入侵。它们所采用的商业防护产品和方案各式各样。然而，并非所有的日常检测都可以发现并确定正在对国家重要经济利益服务造成巨大危害的非法入侵和犯罪行为。

本篇国家计划号召开发并配置计算机网络入侵检测监控系统来发现针对政府机构内部和横跨政府机构的非法或可能的犯罪行为。联邦政府正开发一个综合的框架用于保护这样的计算机系统及其信息的安全性。另外，还对正在进行的有关法律方面的评审提出议案，以期保持对宪法和法律的严格一致性。

**能源部计算机安全战略**

作为能源部的计算机安全巩固项目的一部分，CIO 已经加强了对该部计算机安全的监督。同时，在安全和应急操作办公室的指挥下，CIO 办公室正进行重组。



CIO 官员制定了一个新的计算机安全计划，已于 1999 年 9 月发布。该计划涉及一个关于涉密和非涉密计算机的一致性政策的执行、在 6 个月内一个快速培训活动的部署、一个计算机安全体系结构的构架以及一个计算机安全工具研发项目的开展。

另外，将把位于 Lawrence Livermore 国家实验室的 CIAC（计算机事件咨询功能中心）的工作人员由 7 人增加到 25 人。CIAC 将新承担对安全进行监控以及提供病毒早期预报的责任。

在下两个财政年度（2000 年和 2001 年）中，加强安全工作预计将耗资 8 000 万美元，其中 4 500 万美元用于操作性安全功能的建设开展。

具体时间表见下表：

阶 段	活 动	目标日期
2.4	发布部计算机安全计划，在安全和应急处理办公室管理下重组 DOE CIO 办公室	（1999 年 9 月）

## 2.1 检测入侵及异常行为的防御系统

为了检测到网络上的非法入侵或异常行为，本计划首先号召在关键性联邦系统中安装并实施高度自动化的安全和入侵检测功能模块，包括如下的 4 类防御检测系统：

- 在防火墙两边安装的入侵检测监控器，监控器要定期更新。
- 用于授权用户的访问和活动的规则以及一个检测程序，以确认一个明显的授权用户所出现的异常行为。
- 企业级的管理程序，可以确定网络上有哪些系统，知道它们正在做的工作、加强访问和活动规则并进行安全升级。
- 用来分析操作系统代码及其他软件的技术，以确定是否存在恶意代码（如逻辑炸弹等）以及其他类似于后门等的危险代码（不论其初衷是恶意的还是善意的）。

有必要声明这 4 类安全控制并不是保护网络的必需方案。但是，我们把它们看作是多层构架的、在风险和花费之间达到全面平衡的安全方案的几个重要组成部分。

上面提到的 4 类系统中已有一些进行了商业化。大多数商业程序还是第一代，在很多安装了这类商业程序的系统中，仍需要大量的人工监控以及其他参与。

本计划号召在联邦关键信息系统网络的如上 4 类防御检测系统中的合适地方安装同类产品最优程序。政府可能还将联合私营部门以及各州和地方政府，通过信息共享和分析中心（ISAC）对这类系统做出评价。

## 2.2 用于对攻击数据进行分析及关联的政府级系统

防御检测系统本身并不能提供对关键性联邦系统的足够保护。在现今，几乎所有的应用程序中，入侵检测监控器安装在个人系统或网络上，报警后，系统提交的报告通常比较模糊或者内容过于有限。当一个网络被一种新的技术攻击后，另一个网络可能要花上几天才能知晓这一攻击技术，几个星期后才会得到防御软件，在这期间，关键系统的这种脆弱性一直存在。因此，我们需要一种对入侵数据进行分析及关联的政府级系统，该系统还要具有迅速发布攻击信息的能力。

在目前的防御检测系统的技术水平上，人工管理和分析对于从大量的数据流中综合入侵信息是至为重要的。为了解决这一问题，我们的计划号召入侵检测系统网络以及分析中心进行合作，以对攻击进行检测，任何一个系统被发现受到了攻击，有关攻击的警告词汇立即就可以引起其他站点的注意。

### 2.2.1 政府级系统的三个要素

我们所建议的政府级网络将包含三个参与要素：第一个用于国防部（DoD）和其他的国家安全团体；第二个用于非国防性质的部局（称为联邦民事机构）；第三个向以上两种系统提供信息。目前，这些系统中的两类——JTF-CND 和 NSIRC 已经得到了配置。

- 计算机网络防护联合特别任务中心（JTF-CND）（见第 C 节“目标 2”中的详细讨论）：国防部已经在其中央分析单元内成功地配置了一个网络安全监控器和网络入侵检测系统的联合系统。
- 联邦入侵检测网络（FIDNet）：本篇计划号召在国防部的入侵检测技术以及其他安全技术的基础之上创建联邦入侵检测网络（FIDNet），以保护非国防的联邦系统。该系统由总务管理局（GSA）运行，同联邦各民事机构展开协调。FIDNet 将把覆盖关键性联邦民事系统的入侵检测监控器和一个位于 GSA 的系统异常中央分析器连接起来。
- 国家安全事件响应中心（NSIRC）：负责在国家安全机关需要隔离、控制以及解决危害国家安全系统的事件时对其进行专业协助。

### 2.2.2 协调对入侵检测系统所面临的公共问题的研发

针对用于入侵检测、分析和响应的工具以及技术的不断研发将对于我们在本小节所提出的政府级系统的最终成功有着非常重要的意义。本篇计划号召联邦研发力量对入侵检测进行关注以取得如下目标：

- 入侵检测（ID）报告格式和内容的开放标准：我们需要一种有关途径，使不同的监控器能够共享以公共格式的形式提交的信息，从而便于对这些信息的联合分析。在国防部高级研究计划局（DARPA）的公共入侵检测框架之下，Internet 工程任务组（IETF）已着手此项工作。
- 用于数据分析的自动化及人工智能（AI）工具：我们需要更好的自动化工具来帮助熟练的人工分析员准确、实时地确认入侵。
- 用于系统评估的评估标准/优越性准则：我们需要拥有有效的手段来衡量一个入侵检测系统的性能究竟如何。

### 2.3 FIDNet：一种政府计算机的“防盗警铃”

在文件箱中，人们用锁和防盗警铃来保护重要的信息。FIDNet 就是这样一种用于政府计算机敏感信息保护的防盗警铃系统。

FIDNet 是“系统中的系统”，它将向该系统中的参与机构提供联邦民事级的入侵检测、防范以及响应服务。FIDNet 将把入侵检测监控模块（包括技术和人力）连入到自动化系统中，用来向位于 GSA 的中央分析中心报告数据和系统异常状况。如果出现可能的犯罪活动，FIDNet 工作人员将通过 NIPC 来通知 FBI。

联邦民事机构正在对入侵检测监控器以及熟练的技术人员进行投资。FIDNet 将把各参与机构的模块连到一个大系统中，使这一系统大到一种单个民事机构所无法获得的规模。这包括：

- 位于 GSA FedCIRC 的分析工作班子，将同各机构计算机安全专家合作，评审入侵报告，以及针对未来的可能入侵而提供防范手段的建议。
- 各参与机构和中央分析工作班子之间的安全通信。
- 在软件升级后对其进行验证以消除脆弱性的系统（“补丁”）。
- 为提高系统可靠性和安全性而对系统状态、相关行动所做的更新。

FIDNet 将向联邦系统管理员提供实时的功能模块来分析事件数据，然后对各级系统的安全性和可靠性保障措施做出改进。

### 2.3.1 FIDNet 的优越性

FIDNet 提供了高度集成的联邦民事功能模块以保护关键联邦信息基础设施。它将有助于确保美国政府的正常运行以及全美国人民通信的保密性。预计中的其他优越性还包括：

- 加强了各级系统和联邦机构间对入侵及可疑事件的关联。
- 响应速度有了提高：所有的事件关联和响应均设计成在“Internet 时间”的概念上进行操作。
- 对攻击的检测在时间和空间上都得到了更好的扩展：某些窃取机密的攻击事件，称为“低度飞行者（low flyers）”，其攻击行为尤其低于大多数检测系统的门限（即把它们的网络数据包分散在一个充分宽的范围之内），从而可以躲过检测系统。但范围更为广阔的数据关联以及集中化的数据分析和挖掘将极大地改善入侵检测技术的检测能力，而且这种应用正变得越来越普遍。

### 2.3.2 FIDNet 和对公民隐私与自由的保护

要进行法律方面的评审工作，以确保 FIDNet 的设计、操作以及全面的 FIDNet 观念仍在支持公民的隐私权并符合《电子通信隐私法》（ECPA）及其他的相关法律。

司法部组织的法律预评审认为 FIDNet 的观念严格地符合了 ECPA 的隐私条例（正如其表现出的那样）。正式的法律评审将包括 OMB（管理和预算办公室）及其他联邦机构的参与，目前正在进行。

关于 FIDNet 的其他主要法律观点包括：

- FIDNet 感应器将**不会**监视私营部门的系统或其他非联邦政府所属的系统。该系统只是联邦政府自己的计算机入侵检测网络，而不是在其他大企业运行的网络。FIDNet 的任务是提供一种机制来更好地保障联邦政府**自己**的数据系统和网络的完整性。
- FIDNet **不是**由 FBI 或其他任何执法机构管理的。事实上，它是一种由 GSA（总务管理局）和非国防部的联邦机构管理和提供的服务。

### 2.3.3 FIDNet 的执行

FIDNet 的配置同如下的考虑因素密切相关：

- FIDNet 只是多层的、政府级的信息保护系统中的一个组成部分：对联邦系统的保护需要很多步，包括对人员的培训、标准和操作建议的开发以及每一个部门和机构为改善安全状况而采取的行动等。

- 联合项目管理：在 GSA 的领导下，FIDNet 联合项目办公室将包括一个跨机构的管理小组，其成员来自于国防、情报、技术、执法、隐私管理、立法部门以及消费者机构。它们共同完善系统的参数并向私营部门信息系统安全提供商进行咨询，以开发专用设计参数等。
- 前进中的法律评审：持续的法律评审将确保 FIDNet 的设计和执​​行永远符合隐私权的法律和原则。一个跨机构的工作组，包括各个具有联邦隐私法司法权的机构，正在进行这种评审。
- 研发：要想完成 FIDNet 所有的操作功能，就需要有关注自动化事件分析、可视化、数据挖掘以及网络检测工具的新技术的出现。

内容 2 时间表如下：

阶 段	活 动	目标时间
2.1	在空军、海军、陆军以及国防部建立连接入侵检测系统的分析及响应中心，建立国家安全事件响应中心（NSIRC）	已完成 (1998 年)
2.2	在关键性国防部系统中安装第一批 500 个入侵检测监控器	已完成 (1998 年 10 月)
2.3	建立国防部范围内的 Hub（集线器），用于入侵检测系统——计算机网络防护联合特别任务中心（JTF-CND）	已完成 (1999 年 4 月)
2.5	对联邦系统中的恶意代码进行初步的分析	2000 年
2.6	建立一个用于联邦民事机构的入侵检测网络（FIDNet）试点，到 2000 年 10 月要有 22 个关键性联邦网站连入	2000 年
2.7	对访问/活动监控进行升级，在联邦系统的合适地方建立企业级管理系统	2000 年 10 月
2.8	完成在具有自动化处理和可适应性功能的大型入侵检测网络上伸缩性问题的处理以及其他事项的研发	2000 年 10 月
2.9	开发并定期升级入侵检测系统的标准	2000 年 10 月
2.10	在联邦政府需要的地方对防火墙和入侵检测监控器进行升级	2001 年 1 月

内容 3：建立、维持、协调稳健的执法手段以及情报功能，以保护关键信息系统，保持与法律的一致

围绕着国家基础设施保护中心（NIPC），联邦政府正在开发一套用于向国家提供实时攻击威胁警报及响应的系统。该系统的其他组成部分是 FedCIRC、情报共同体以及 NSIRC。国防部的 JTF-CND 也是其一部分。这一系统还需要私营部门中的信息共享和分析中心（ISAC）的补充，对此的讨论见私营部门计划部分。

### 3.1 国家基础设施保护中心（NIPC）

PDD63 授权 FBI 内先前的组织——计算机调查和基础设施威胁评估中心扩张成为一个大规模的国家基础设施保护中心（NIPC）。PDD 中说明 NIPC “应该成为一个国家的关键基础设施威胁评估、预警、脆弱性及执法调查和响应实体”，并且进一步声明 NIPC 的任务“将包括提供及时的国际威胁警报、综合性分析以及执法调查和响应”。

PDD 把 NIPC 放到了对威胁和攻击的政府预警、威胁调查以及响应这一系统的核心位置。NIPC 是收集基础设施的威胁信息和“促进和协调联邦政府对事件的响应”的焦点机构。NIPC 还负责“减轻攻击后果、调查威胁以及监督重建工作”。然而，PDD 还进一步说明，根据国外威胁/攻击的性质和水平、各特殊职能机构〔司法部（DOJ）/国防部（DoD）/中央情报局

(CIA)] 之间制定的协议以及最终的总统决议, NIPC 可以被放到直接支持国防部或情报共同体的位置上。PDD 进一步规定了 NIPC 应该包括“负责报警、分析、计算机调查、协调应急响应、培训、推广以及技术工具开发和应用的各个组成要素”。

NIPC 担负着从所有相关资源处收集和传播信息的重要作用。于是, PDD 要求 NIPC “在进行分析并将报告以合适的格式提交给联邦以及各州及地方政府、关键基础设施所有者和运营者、私营部门信息共享分析实体之前, 对执法和情报信息做出过滤处理”。NIPC 也负责“向任何私营部门信息共享和分析实体以及所有者和操作者”发布“攻击警报或危险状况恶化的警戒通知”。

为了完成这些目标, NIPC 正在广泛的政府和私营部门实体中建立一个关系网。PDD 考虑了几种途径。第一, 它指明中心将“包括 FBI、特工处的代表以及其他对计算机犯罪和基础设施保护具有丰富经验的调查者, 还包括具体从国防部、情报共同体、指挥机构来的代表”。第二, NIPC 将“同政府的其余部门, 包括预警和运营中心以及任何私营部门信息共享中心实行电子化方式的连接”。第三, 所有的行政部门和机构被要求“同 NIPC 合作, 在法律允许范围内应其需要给予帮助, 提供信息和建议”。第四, 所有的行政部门和机构也被要求“在法律允许的范围内共享 NIPC 提供的关于攻击威胁和预警以及对关键政府和私营部门基础设施实际攻击的信息”。为确保这些信息不被阻碍, 在处理计算机攻击时, 这类信息是刻不容缓的, PDD 授权 NIPC “建立其自己同私营部门的信息共享和分析实体的直接联系”。NIPC 分为 3 个部门: 计算机调查和操作、分析和预警以及培训、推广和策略。

作为本篇国家计划中其任务的一部分, NIPC 将做如下工作:

- 对基础设施运营者的推广: NIPC 的培训、推广及策略部门正制定一个综合性的推广计划和针对每类基础设施的二级计划, 该推广计划中将开展这一工作以及 PDD63 中提到的特别推广任务。计划中含有种种推广活动, 包括联邦机构、法律实施部门以及 DoD 同私营部门的接触; 向企业和工业协会领导的推广; 同其他已和私营部门建立联系的各级政府和准政府实体之间的合作等。推广计划的目的是把 NIPC 与现有的政府部门-私营部门互作用的机制和途径连接起来, 并在没有这种互作用机制的地方对推广资源进行关注, 从而创建这种机制, 最终在 NIPC 和每个基础设施之间建立起高效的信息流。部门联络官和部门协调中心将同 NIPC 协同工作以执行这一推广计划。

NIPC 正开发 KAI (重要资产行动) 项目。KAI 将建立并维护每个基础设施部门 (比如高压输电网、通信交换节点等) 中特殊“重要资产”的数据库, 并维持和每一资产的“接触点 (point-of-contact)”。KAI 的目标是:

- 确定并把重点基础设施资产输入数据库;
- 建立同资产所有者和操作者的 POC (接触点) 及联络;
- 协助应急计划的制定。

如果服务或产品的丧失及失败会导致影响广泛且严重的社会经济后果, 那么提供这些服务或产品的单个组织、组织集团或者系统都将被视为重要资产 (列为 8 类关键基础设施部门之一), 从而成为 KAI 的目标。

最后, 项目将包括对每一司法机构和示范单位的响应计划做出演习测试, 以决定一次攻击对特定资产造成的影响。FBI 区域办公室 (FBI 在国家各主要区域的负责组织——译者注) 将负责制定各自管辖权限内的资产列表, NIPC 负责维护这一国家数据库。项目将在与部门

协调中心、部门联络官、国防部以及其他机构的协调下开展。因为重要资产对于物理和计算机攻击都存在脆弱性，所以 KAI 以及相关的响应计划对这两种攻击都会考虑到。而且 NIPC 将会同国家国内战备办公室（NDPO）密切合作，确定对基础设施的物理威胁。

- **InfraGard 项目：**NIPC 正在建立同工业界的有效通信线路，用于实现威胁预警和其他信息的共享。InfraGard 项目的设计希望在国家和地方的级别上均实现私营和公共部门的信息共享机制。它的目标尤其在于：
  - 为各成员提供迅速、有价值的威胁咨询、预警和警告；
  - 增加提交给地方级 FBI 区域办公室（用于协调、调查以及追究）和 NIPC（用于国家级的分析和警告）的基础设施威胁信息以及事件报告的数量和质量；
  - 改善 InfraGard 成员、相关的地方 FBI 区域办公室、NIPC 之间关于基础设施威胁、脆弱性和互依赖性的相互作用和信息共享；
  - 遵循所有权、法律和安全要求，对 InfraGard 成员、相关的地方 FBI 区域办公室、NIPC 之间所共享的数据进行防止计算机及物理性威胁的保护；
  - 为各成员提供关于基础设施脆弱性和保护措施的教育和培训论坛。

在 2000 年，FBI 将在全国范围内扩展 InfraGard 项目。这种扩展包括：安全报警网站的开发，从而为各成员提供有关最近入侵的信息；对基础设施保护的研究；成员间安全通信的能力保障等。这将使 NIPC 迅速获得美国工业的有关受攻击信息并立即采取响应。这一项目旨在对部门联络官和部门协调中心建立的威胁预警网络所发布的报警信息进行补充和放大。

- **脆弱性评估/分析以及信息共享：**分析和信息共享处将负责分析所有的资源信息。基础设施分析（如各部门依据 PDD63 所做的评估）、威胁分析（如情报共同体做出的他国或恐怖主义集团威胁分析）以及最近的情报（来源于调查机构、管理机构或私营部门的报告）都将汇总在一起，产生基础设施险情评估。这些评估形成了各类成果，包括预警和咨询、《基础设施保护摘要》以及各种主题电子报告的基础。这些成果将通过监察与预警处向政府和私营部门层层分发。NIPC 将在 2000 年首先从电信部门和能源部门开始进行险情评估。
- **观察和预警：**观察和预警处（WWU）负责监督所有的资源报告，它是信息的收集点。WWU 将从开放资源、当前调查、情报资源以及其他机构处收集和传播计算机入侵和与基础设施有关的信息，也可以从各种各样的 CERT 和任何与 NIPC 合作的私营部门信息共享和分析中心（ISAC）处获取信息。NIPC 将起草并向联邦政府、各州、地方执法部门及私营部门等传播这些涉及计算机威胁和事件的预警以及告诫。当恐怖主义集团可能成为威胁事件的组织者时，它将会同 FBI 的恐怖主义威胁警告系统合作。WWU 的目标就是，确保所有的关键基础设施资产都已经及时地得到了关于威胁警告、报警以及告诫的通知。

由 WWU 收集的信息将被立即分析以确定大规模的攻击是否已经开始。如果 NIPC 确定了一次攻击正在进行，那么它可以使用一整套机制向联邦政府和私营部门的适当团体发出已过滤和未经过滤的预警，使它们可以采取及时的保护措施。这需要对报告和过滤的步骤进行设计，还需要信息收集和发布的机制，因此不是一个简单的过程。NIPC 目前正在对这些步骤和机制进行研究。

NIPC 还负责改善电信线路以促进威胁预警向工业和所有政府机构的发布。通信所依赖的现有机制包括执法在线和国家执法通信系统（NLETS）来通达各州和地方执法部门。其他的机制有：NIPC 的 Web 主页、国家安全意识发布和响应系统（ANSIR）以及可以到达联邦、各州及地方政府和一般公众的其他机制。NIPC 将继续研究开发新的途径使预警和威胁咨询能够到达不依赖于上述实体进行通信的实体。NIPC 的长期目标是开发一种尽可能利用所有现有通信机制的综合预警系统。

当 NIPC 成熟后，WWU 将继续确认其他合适的咨询和预警接收方，继续做出对其所收集到的最重要信息进行强调的每周报告（如上所述）。NIPC 工作人员正在制定一套用于私营部门和政府实体间信息共享以实现相关信息和分析传播量最大的指导方针和方法。NIPC 计划中包括了对 WWU 的重新选址——它原来和 FBI 的扩展后的战略性信息和运营中心相邻，还包括把国防部和情报共同体的分析并入 NIPC 之中以及获得其他的技术资源。目前，WWU 保持着对一般操作进行的每周 5 天、每天 16 小时的监察频率。一旦其他的政府机构人事安排上马，它就计划在 1999 年以每周 7 天、每天 24 小时的频率工作。在这之前，如果发生任何危机事件，它将使监察中心立刻投入 24/7 的运行频率之中。

- 计划制定和协调活动：NIPC 正在协调执法部门保护计划的制定。已经指定了相应的部门协调中心，部门的时间计划也已制定并提交给了 CIAO。
- 计算机威胁调查和响应：NIPC 提供了促进并协调联邦政府对关键基础设施攻击事件进行响应、减弱攻击、调查威胁以及监控关键性计算机资产重建的手段，包括政府所依赖的电信和计算机网络。NIPC 是协调危机管理、响应关键基础设施攻击的政府领导单位。

NIPC 的国家任务已经被引入进了一个新的调查性项目中，称为国家基础设施保护和计算机入侵项目（NIPCIP）。该项目包含在 FBI 反恐怖主义处中。NIPCIP 小组在 FBI 区域办公室中负责实施对计算机入侵的调查并对威胁做出响应，同时依照《国外情报收集和国外反情报调查司法部长指导方针》进行情报收集工作。在 10 个大城市的区域办公室内，FBI 设置了计算机犯罪小组。而且，每个办公室内还包括一个 NIPCI 小组。在未来的几年内，FBI 的目标是在所有的区域办公室中设置 NIPCI 小组。

作为危机管理模块一部分，NIPC 能够对可能的违法、危害国家安全或危害国家基础设施的事件做出响应。NIPC 的工作人员具有非常高超的计算机和信息安全技术及知识，还具有熟练的犯罪调查和国家安全调查经验。NIPC 的目标是对于最初的危机迅速反应、依据事件的性质施以适当的法律措施或国家安全战略。为此，NIPC 成立了一个网络应急支持组（CEST），一旦人员配备完成，就能立刻投入部署。

- 培训负责基础设施保护的联邦、各州以及地方级别官员：FBI 计划在 NIPC 和各区域办公室的管理层中增加受过技术培训的调查员的人数。1998 年，NIPC 在其他执法部门中培训了 170 名 FBI 特工和 17 名代表。计划在 1999—2000 年度培训超过 500 名执法人员（联邦、各州以及地方上的）。其他培训机会包括由各私营部门提供的信息安全专业课程等。FBI 还正在扩展其计算机法学项目，并在每个区域办公室设置了至少一名全职的计算机法学检查员。

在与 NDPO（国家国内战备办公室）的联合下，NIPC 将推广其对地方上的第一时间响应人员以及州和地方基础设施执法部门的培训工作。NIPC 正在试图培训美国 50 个州和哥伦比

亚特区中任何一个州政府级调查机构中的调查员，并在每一州级调查机构中培训至少一名培训师。NIPC 还试图培训重要城市首脑协会代表城市和重要郡县警长协会中的调查员，而且已经就此事向国际警察首脑协会和国家郡县警长协会做了咨询。更大规模的培训包括在一门 1999 年发起、跨时 1 周的实用课程上培训出 500 名州和地方执法部门人员。

NIPC 正制定其演习项目以测试美国政府各机构和基础设施部门操作员在面临基础设施危机时的反应。1999 年间至少开展 1 次演习项目。

### 3.2 FedCIRC（联邦计算机事件及应急响应功能中心）

我们对于跨机构的事件处理功能的需要从来没有像现在这样强烈过。位于总务管理局（GSA）的 FedCIRC（联邦计算机事件及应急响应功能中心）是一个由计算机事件响应专家、安全专家以及执法专家合作组成的机构，用于处理计算机安全事件并为联邦政府提供事前和事后的安全服务。

FedCIRC 的首要目标是，提供相关的途径，使各联邦机构能够实现合作以共同完成下列事项：处理安全事件；共享相关信息；解决共同的安全问题；同 NIPC、JTF-CND 以及 NSIRC 协作。这种机构间合作的焦点是为未来的基础设施保护战略制定计划并处理威胁到关键信息基础设施的犯罪活动。

FedCIRC 通过如下手段来完成其目标：

- 向联邦民事机构提供技术信息、工具、方案、协助以及指南；
- 提供联络和分析支持；
- 通过与联邦民事机构、国防部、学术机构以及私营工业建立的合作关系，鼓励高质量产品的和服务的开发；
- 提高政府 IT 资源最高安全轮廓；
- 提高联邦政府内的对事件响应和处理流程的认识；
- 为有效防止、检测、处理计算机安全事件并进行有效的事后恢复，培育各联邦机构间的合作关系；
- 提供通信手段，使关于潜在威胁、事件状态的报警和劝诫信息能够传达；
- 增强其他联邦机构的事件响应能力；
- 促进与安全相关的信息、工具以及技术的共享。

FedCIRC 的合作系统已经一致同意将其收集、编纂并分析过的信息进行交流，使联邦政府能够保护其资源，防止针对关键性信息处理系统的攻击或者在事后能对资源进行迅速恢复。

### 3.3 情报共同体在信息共享中担当的角色

情报共同体（IC）由 13 个机构或其下属单位组成，其保护信息系统的活动多种多样。

IC 对保护整个联邦政府和国家的信息系统起着重要的作用，它的任务是收集、分析并发布关于国外威胁的情报。这既包括外国政府和非政府部门的计划、意图等战略性信息，也包括攻击即将发动（即预警）和攻击正在进行的战术性信息。国家已经建立了向国防部和包括 NIPC 在内的其他联邦用户发布这些情报的机制。IC 支持最大可能的信息共享，在保护其资源和工作方法的限度内发布所有可能的情报。

另外，IC 各机构还对 NIPC 的工作进行支持，包括收集基础设施威胁信息、改进并协调联邦对于事件的响应、减弱攻击、调查威胁以及监控事后重建等。IC 官员被选派到了 NIPC



去，以促进信息共享并征集各种要求。NSA 负责很多联邦信息安全工作，它将对特别事件中的数据进行分析，从而给予 NIPC 进一步的支持。

3.4 国家安全事件响应中心（NSIRC）

NSIRC 是 NSA 为了对付给美国政府的国家安全信息系统造成巨大冲击的计算机事件而成立的焦点机构。NSIRC 可以实时地发布美国信息系统的威胁警报，向国防和民事机构提供专业帮助，从而隔离、控制以及解决对国家安全系统造成威胁的各类事件。

NSA 向其客户/合作者提供的服务是独一无二的，因为它有能力对严重的入侵事件进行深度的技术分析，而且它是唯一可以把入侵数据同外国信号情报<sup>①</sup>进行联合，从而实施分析的机构。NSIRC 将提供计算机攻击威胁警报以及技术响应，其目标是基于关联和融合后的信息做出威胁和脆弱性的实时报告，并把这些报告向其客户/合作者提供，另外，还通过计算机诊断法为这些客户和合作者提供专业技术分析报告。

NSIRC 将把其分析及开发力量投入到国家级的网络防御实体上，如 NSC、NIPC、JTF-CND、DISA（国防信息系统局）以及 FedCIRC。NSIRC 如今管理着一个包含国防部及很多民事机构计算机攻击事件的数据库。从 1998 年到现在，该数据库记录了 5 700 次计算机攻击事件，攻击源头既有国外的也有国内的。NSIRC 基于这一数据库来发布警报和威胁咨询，警告政府网络防御机构注意那些有可能是系统攻击源的 IP 地址（即“坏地址”），或者注意新的或已有的黑客组织以及不同寻常的黑客攻击行为等。

NSIRC 由 4 个部分组成，它可以借助 NSA 中的任何部门来支持网络防御的需要。4 个部分分别是：信息保护单元，在 NSA 的国家安全运营中心内，每周 7 天、每天 24 小时运行；网络利用报告和分析处，提供网络事件的全面资源分析；网络入侵分析功能部，提供计算机诊断分析，向客户介绍尽可能详细的黑客入侵技术；最后，还包括一个威胁评估处，为美国电信和信息系统提供全方位的威胁评估。

内容 3 时间表如下：

使执法、情报部门及其他联邦组织共享脆弱性信息、威胁信息以及预警的活动时间表

阶 段	活 动	目标日期
3.1	提高联邦执法部门和情报机构对于收集、追踪以及分析计算机威胁和关键信息系统脆弱性的关注	已完成 (1999 年)
3.2	情报共同体、国防部以及联邦执法部门发起一系列工作组来开发新的适于对付计算机威胁的信息收集技术以及分析技术	已完成 (2000 年)

内容 4：快速共享攻击威胁警报和事件信息

信息经济极大地依赖于高度互联的系统。恶意入侵不仅仅限于攻击单个系统；病毒可以通过多个网络快速传播。为了有效地对付这些威胁，国家需要一个能够快速共享关于现行入侵或可能入侵的信息的系统，该系统还要能够使即将到来的计算机攻击的迹象信息和抵御攻击的方法得到快速共享。

① 指通过对截获的信号进行分析而破译出的他国情报，最早始于中途岛海战。——译者注

联邦政府在此时的角色包括既要提供联邦的信息共享功能，也要鼓励非联邦实体（私营部门以及州和地方政府）组织起来实现有关攻击威胁和事件信息的高效交流。特别是，联邦政府将：

- 继续巩固 NIPC 作为联邦信息共享中心的角色；
- 鼓励私营部门信息共享和分析中心的开发（ISAC）；
- 通过 FIDNet、NSIRC 以及 JTF-CND 自动共享联邦政府间的高度可疑事件以及攻击数据。

#### 4.1 巩固 NIPC 作为联邦威胁和预警信息共享中心的角色

当前，我们需要对入侵、威胁以及非授权攻击的信息做更多更好的处理工作。通常是系统管理员第一个发现非授权入侵和攻击的迹象，在联邦政府和私营部门中都是如此。系统异常和其他事件数据可以视情况发给各 ISAC（私营部门中）、FIDNet（联邦民事机构）以及 JTF-CND（军事机构）。而且，根据 PDD63，私营部门和美国政府实体还均应就这些信息直接同 NIPC 或当地的 FBI 区域办公室联系。

提供给 NIPC 的非授权入侵和攻击的信息可同情报、执法方面的信息以及开放资源和 NIPC 所掌握的其他信息结合在一起。对所有的资源信息作集成和分析时将考虑到对那些无法仅由技术手段就能完成的入侵行为和模式的检测。

联邦系统已经成为了很多入侵行动的首选目标，因此，对涉及联邦系统的入侵事件进行充分分析并做出能被广泛共享的深度结论就成了当务之急。国家计划号召继续加大步伐以确保有关联邦计算机系统遭非法入侵的情况能够汇报给 NIPC，并能得到恰当的共享。还要努力满足下述要求：

- 所有的行政机构都应该同 NIPC 共享有关威胁和警告的信息以及针对政府和私营部门关键基础设施而发动的现行攻击的信息。
- OMB（管理和预算办公室）和各机构的 CIO 对于向 NIPC 提交事件信息应持有明确的指导方针，还应对系统管理员进行培训，这些措施将提高消息的数量和质量，从而便于分析和结果共享。
- 在 FedCIRC、其他的联邦计算机应急响应中心（各 CIRC 和 CERT）以及 NIPC 之间实现有效的协调，这将促进联邦系统事件信息的完全共享。CIAO 和 GSA（管理 FedCIRC 的机构）将在 2000 年为各联邦 CIRC/CERT 召开一次白宫会议，推动各组织间的协调和公共操作标准的发展。

NIPC 将持续发布分析结果并使其得到共享。这些分析结果不但包括 InfraGard 报告，还包括每日报告和双周报告以及威胁状况特别通知。

#### FAA 计算机安全事件响应功能中心（CSIRC）

FAA（联邦宇航管理局）计算机安全事件响应功能中心（CSIRC）是一个集中化的报告和监控功能中心，它将确认、评估信息系统安全（ISS）事件并对其做出响应。CSIRC 功能体将横跨各类 FAA 商业线路，为所有类别的 FAA 信息系统 [国家空间系统（NAS）、任务支持或管理系统] 提供保护。它的三个主要功能是事前措施、事件报告和响应以及灾

后恢复。1999 年建成了初步的运行能力，2000 年将在少数几个系统中建立全面的运行能力，在未来的几年中，将加大投资以在所有的 FAA 信息系统（NSA、任务支持和管理系统）中实现全部功能。

#### **事前措施**

通过与其他部门和组织中的类似功能机构的协调，CSIRC 将发布与 FAA 系统有关的咨询、公告以及报警。同时，向 FAA 办公室提供技术协助也属于此类措施的范畴。

CSIRC 将负责 FAA 范围内的入侵检测并由 FAA 管理机关授权对所有进入 FAA 设施的网络行为进行全天候拦截。CSIRC 将监控和分析入侵检测的数据以确认安全弱点和非授权活动。

#### **事件报告和响应**

CSIRC 将充分地利用计算机事件响应小组（CIRT）。这个小组在处理入侵和计算机事件方面受过专门训练，它由计算机专业人士、计算机技术科学家、工程师和现场系统专家组成，为系统管理员提供电话帮助，而且必要时可以赶赴现场协助进行灾后系统恢复。区域现场系统专家精通于对影响 NAS 的区域紧急事件和故障进行响应，而且，就其本身而论，这是 CIRT 任务的主要部分。

#### **灾后恢复**

CIRT 将提供灾后恢复帮助。它将对所有破坏进行评估并记录。

### **4.2 推动 ISAC 的建设**

本篇国家计划号召并鼓励为私营部门和州及地方政府建立信息共享和分析中心（ISAC）。ISAC 将在各公司以及州和地方政府间实现信息共享，或从政府处接收警报信息。

对于愿意建立 ISAC 的公司和非联邦实体来说，ISAC 是一种向联邦机构通知攻击信息的自愿性机制。在通知联邦机构前，ISAC 可以事先“过滤”这些数据（比如，把受攻击目标的名字删去）。然而，我们鼓励各公司把攻击数据直接报告给 NIPC。

联邦政府在 ISAC 的建设中担当如下一些角色：

- 共享威胁和脆弱性数据及攻击信息：联邦政府对于确认和矫正脆弱性具有深刻的洞察力以及丰富的经验，对入侵反应具有熟练的技术。联邦政府的这些信息将在各可信非联邦实体间共享，例如 ISAC。这些可信非联邦实体将利用这些信息改善私营部门和州及地方政府的计算机安全性。
- 法律变革：很多公司愿意和联邦政府或其他公司共享安全信息，但它们在考虑到信息保护或由此产生的责任时则往往望而却步。欲组织 ISAC 的公司在反托拉斯因素下也会打消其念头。很多公司尤其担心其透露给政府的信息会在《信息自由法》（FOIA）的要求下被迫向公众透露。于是，在 1999 年 7 月 CIAO 和司法部发起了一次白宫会议，专门来探讨这些问题。当前，一个工作组正在研究确保私营部门信息保密性的解决方案。

还有另外的类似工作也在开展，这些工作希望能开发出可以解决私营部门上述顾虑的方案。

- 启动支持：认识到某些私营部门在建设 ISAC 时需要支持，处于领导地位的联邦各机构将在 2001 年的预算中拨出一部分用于协助 ISAC 建设。但是，联邦政府对 ISAC 启动的任何支持在规模和时间上都是有限的；ISAC 的用户——私营部门和州及地方政府，必须愿意对 ISAC 提供必要的长期支持。

#### 4.3 通过 FIDNet 和国防部的 JTF-CND 进行信息共享

在现有的技术下，系统异常（恶意入侵的征兆）的分析主要基于人力，系统范围内的响应也是如此。持续的研究和开发是 FIDNet 的重要工作，旨在开发自动化和人工智能工具，提高事件分析的速度和准确性。

另外，随着以后的发展，对攻击的洞察将更为深入，不仅仅只是提供攻击的事实，还有可能需要提供攻击的过程、采用的技术以及摧毁攻击的途径等信息。分析单元将能够开发出系统“补丁”来阻挡攻击。通知和响应等过程，包括补丁的安装，最终将在很大程度上实现自动化。

根据隐私和执法要求的许可，FIDNet 和 JTF-CND 的事件检测系统将同 FedCIRC 一起共享事件数据。如果事件数据表明需要采取法律行动，那么这些数据将会被交给 NIPC。

内容 4 时间表如下：

阶 段	活 动	目标时间
4.1	司法部和 CIAO 在白宫会议中心召开一次关于信息自由法和保护关键系统脆弱性信息的会议	已完成 (1999 年 7 月)
4.2	在 NIPC 建立 24 小时的全天候计算机攻击通知功能模块	已完成 (1999 年)
4.3	开发用于同私营部门的 ISAC 进行安全信息共享的机制	2000 年
4.4	CIAO 和 GSA 将为各联邦政府的 CIRC/CERT 发起一次白宫会议，推动这些公共运行系统的协调和发展	2000 年
4.5	提交法律方面的革新议案（如果需要），以帮助 ISAC 的建立	2000 年
4.6	和私营部门集团合作，在几个重要工业中建立 ISAC	2000 年及以后
4.7	在州级别上并同多个州级权力机关一起创建测试床或计算机安全信息共享流程的样板	2000 年
4.8	建立其他的信息共享和分析中心	2000 年

#### 内容 5：国家范围的响应、重建和恢复系统

信息战攻击的规模大小不限。攻击可能作用于整个公司或机构，也可以是整个经济部门，还可以是国家的某一区域甚至国家本身。根据从 JTF-CND、FIDNet 和工业集团的 ISAC 处得来的攻击数据，NIPC 将和联邦机构以及私营部门合作以确定一个正在进行中的攻击的规模。

一旦一次广泛的攻击得到确定，中心将和执法部门及其他相关机构一致合作来响应该攻击，包括向系统管理方发出建议，从而：

- 阻断可疑用户的访问通路；
- 实行特殊“防御状态”安全警戒；

- 针对攻击采用的技术，应用新的安全软件“补丁”；
- 隔离网络的某些组成部分；
- 中止某些网络运行；
- 启用紧急事件下的接管系统。

与此同时，执法部门和其他相关机构将对攻击源进行定位并采取合适的措施将其中断。我们鼓励私营部门和执法部门之间就攻击响应行动多做磋商，以免私营部门的行动对入侵调查造成不必要的阻碍，防止抹掉入侵者的属性特征甚至耽误对侵略者的起诉。

政府的目标以及我们对工业界的建议是，每个关键性信息系统都要准备响应计划，这些计划中要包括为如下响应行动所作的准备：迅速启用其他的防御措施（如更为严格的防火墙要求）；在某些预定情况下关闭部分网络（通过企业级的管理系统）；把最小化基本操作交由“干净”系统运行；迅速重建受感染的系统。

在很多情况下，企业和机构的恢复计划只集中于或主要集中于物理破坏：洪灾、暴风雪或爆炸等使总部瘫痪的事件。在这些计划中，作为替代的总部将接替原总部的运行，仍继续把各种指令发往各公司或机构的信息系统网络中。现在这些计划中通常包括“备份”计算机数据库，用于在总部系统不存在或无效的情况下。

如今，恢复计划还必须能够应付所有或部分信息网络本身被破坏的情况。这时，一定要有替代的方法用来传送最小量的重要信息。专家组要立刻赶到以协助重建工作，包括分析导致网络瘫痪的软件错误以及设计代用方案，还要负责网络重启。

### 5.1 建立在 Y2K 事件（“千年虫”）的防御基础之上

2000 年计算机系统转换及关键信息系统保护计划对国家迅速掌握重建关键性计算机系统的能力提出了要求。千年虫防御的计划者们为那些在千年的过渡期有可能出问题或被攻击的关键基础设施系统做了很多准备。一个联合了联邦政府和私营部门的资源的国家系统得到了创建，目的是在千年过渡时监控、协调和帮助重要计算机系统的重建，如果有必要的话。

这个国家级的重建系统是对联邦响应计划的补充。在联邦响应计划中，联邦应急管理局（FEMA）被指派为应急处理设施的领导机构，在总统宣布国家进入紧急状态后负责全面的灾后管理事项。联邦响应计划涉及了 Stafford 法案以及其他的相关法令。但是，这些机制没有谈及对那些受到计算机攻击或在千年虫问题中受影响的信息系统的重建。这些联邦响应机制仅仅是为处理计算机事件中的物理和社会后果而设计的。

我们需要对联邦响应计划的机制做出补充，那就是，我们的国家要具备一种在巨大破坏发生后仍能维持政府和私营部门重要系统运行的能力。

2000 年过渡和国家协调员总统会议主席汇集了各方的努力来发展这种重建能力。总统委员会建立的信息协调中心（ICC）与关键基础设施保障办公室以及其他致力于保护关键基础设施的研究所进行了密切合作。在 PDD63 中，总统曾号召建立公共-私营部门的合作关系来保护国家的关键基础设施。CIAO 负责协调这篇国家计划的发展并分析联邦政府对各关键基

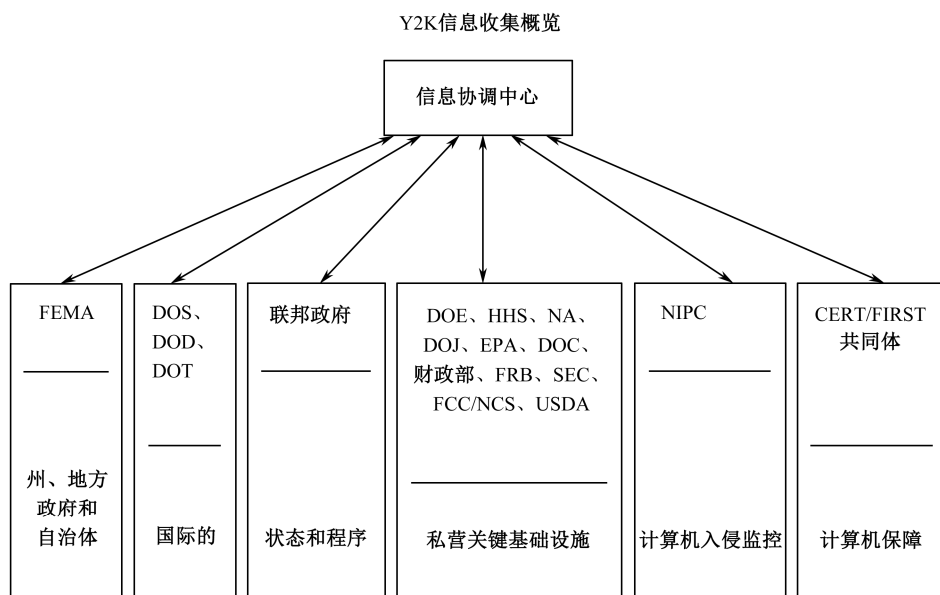
基础设施的依赖关系，还处理政府内的有关法律和公众事务，另外，相关的教育和培训活动也由其负责。于是，安排 CIAO 和 ICC 之间的工作力量就成了我国千年虫防御工作的主要部分。

千年虫防御系统的主要组成部分如下。

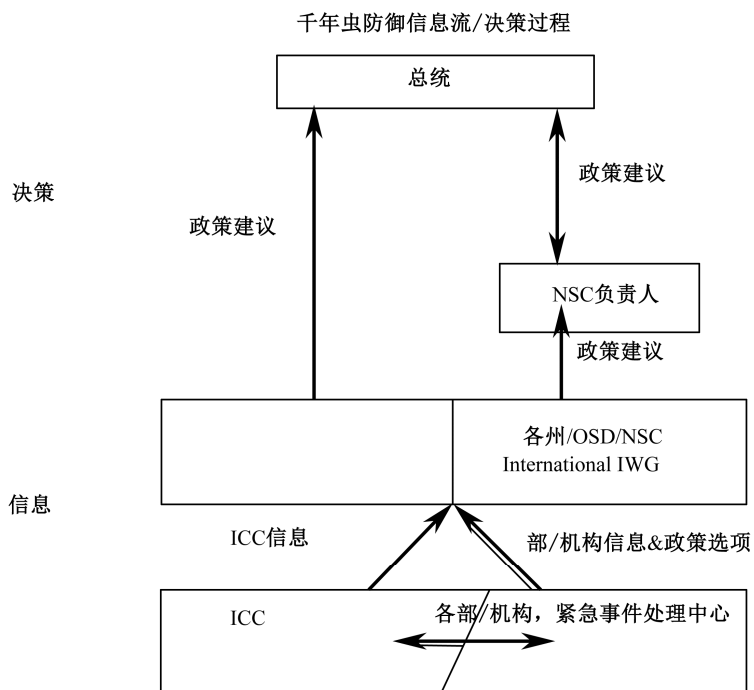
- 信息协调中心 (ICC): ICC 的工作包括在联邦政府和公共及私营部门的主要实体间实现信息共享; 协调各机构对可能给国内外美国利益造成负面影响的千年虫事件相关活动所进行的评估。
  - 不论是公共还是私营部门, 在 2000 年的过渡过程中均有一定的信息需求。ICC 负责报告联邦重要计算机系统和关键基础设施在 2000 年过渡期的运行状态。另外, ICC 还报告国内外主要部门中的联邦机构及部门工作组所确认的关键系统的运行状态。
  - 这一报告系统的主要特点是 ICC 和基于私营业的各个国家信息中心 (NIC)。在千年过渡阶段, 超过 14 个 NIC 提供了主要工业领域的相关活动细节。这些 NIC 涵盖了零售业、航空运输业、天然气工业、食品生产工业以及能源工业等领域。专为千年过渡而建立的计算机保障 NIC 包括了计算机元器件业、计算机安全和 Internet 等领域, 它致力于 Internet 的蓬勃发展, 并努力发展同外界的关系以对其他的关键基础设施提供支持。
  - 如果在千年过渡阶段发生了严重事故, 则 ICC 将收集各机构的紧急状态报告、监督各部门的响应, 并在合适的范围内帮助对重建功能的协调。这些能力包括建立资产的清单、整理各类资源以及促进信息共享。信息收集活动有助于保护生命、财产和关键基础设施系统。ICC 尤其关心有可能严重影响国家利益或公众健康及安全的千年虫紧急事件。
- NIPC 响应协调: 千年过渡过程中, 在与信息协调中心的密切合作下, NIPC 随时准备协调情报和执法功能, 以响应犯罪和国家安全威胁。如果发生了国家范围内的重大事件, 则 NIPC 在 PDD63 的授权下可以监控重建工作, 从而确保响应和重建的协调。
- NIPC 在 2000 年问题中的角色: 在 2000 年问题中, NIPC 始终保持对计算机威胁或其他事件的实时警惕, 并向合适的政府部门和私营部门团体发布预警, 协调政府对这些事件的响应。
- 重要部门的网络资源: 建立在业已进行的重建准备工作的基础之上, 千年虫事件 (Y2K) 委员会和 ICC 与工业协会和其他团体协同工作, 鼓励在每个经济部门内建设专家小组中心。这些高度私有化的工业部门响应中心可以给予很多专家建议和资源帮助。
- Y2K “黄页” 和重建资源: 建立在业已存在的资源材料和千年事件援助者提供的“黄页”的基础上, 随着与 CIO 委员会的密切协调, ICC 鼓励资源指南的开发, 向 Y2K 响应者提供重建信息。

对千年虫防御的经验全面分析之后, 它的重建功能可以被我们所利用。通过与其他政府机构以及私营部门的协作, 我们可将其发展成一个持久性的国家计算机重建功能模块, 在与 NIPC 的协调下对主要的计算机入侵事件做出响应。

千年虫防御机构的组成如下图所示:



千年虫防御信息流/决策过程如下图所示：



## 5.2 集成计算机响应、重建和恢复操作的连续性

在 PDD67 中，总统要联邦各个部和机构在 1999 年年底之前提交新的连续性操作计划。这些计划要包括在信息战攻击时能够确保运营连续性的措施。

联邦部门联络官将同各自对应的工业界合作，确保企业的恢复计划中也同时提及了信息攻击重建。跨机构的基础设施保障办公室（CIAO）将发起一次有保险业和审计业参加的白宫会议，并同它们开展持续的对话，以促进对风险管理、操作建议以及衡量标准的理解。

响应、重建和恢复时间表如下：

阶 段	活 动	目标日期
5.1	各部和机构将修改其运营连续性计划，考虑意外事件以及 PDD63 中谈到的紧急事态	已完成 (1999 年 12 月)
5.2	CIAO 将发起一次由审计和保险业的代表和部门协调中心参加的白宫会议，会议集中关注商业控制和审计界在信息时代的新角色	2000 年
5.3	JTF-CND 以及其他政府机构将为政府信息攻击报警网络开发协议和建议	2000 年
5.4	FEMA 将进行应急通信系统的现代化改造	IOC: 2000 年 FOC: 2003 年

## 内容 6：加强基础设施保护中的研发

### 6.1 关键基础设施保护研发活动

关键基础设施保护研发活动（CIPRDI）扩大了基础设施保护中的联邦研发的范围和资金。CIPRDI 还通过关键基础设施保护 R&D 跨机构工作组（由白宫科技政策办公室领导）第一次协调了联邦政府在该领域内的工作。

CIPRDI 将在 5 个主要的横向领域扩展联邦政府的研发工作，这些工作将直接支持所有关键基础设施保护中的各部门的特别研究需求。有两个 CIPRDI 项目优先级最高，其中之一是开发自动化工具，用以检测陷门和其他恶意计算机代码，另一个是开发对系统异常行为报警的相关技术。

#### （1）脆弱性和风险评估

- 开发脆弱性检测、评估以及分析工具：该研究的第一目标是确认、收集、组织以及发布基础设施脆弱性信息。第二目标是研究在基础设施的设备和系统，包括硬件和软件开发以及集成过程中避免、减少或消除脆弱性的技术和方法。预期结果包括威胁和脆弱性信息字典、脆弱性和攻击分类方法及分类数据库以及脆弱性分析技术和方法。
- 开发用于风险管理、性能评估、安全测试的高级工具和评测基准：该项研究将开发新的基准和衡量工具来对基础设施性能等参量作实时测量，这可以在基础设施出现重大问题之前就检测到其性能的下降。
- 特征化威胁及通告：该项研究关注信息与通信基础设施的数据收集和分析。特别地，这些信息将用于对威胁进行动机和源头的特征化，从而开发出可以描绘攻击者并精确定位攻击源的工具和技术。

#### （2）信息保障

- 开发高级信息保障工具：该研究将为硬件和软件组件以及他们在系统中的后续集成而开发相关工具和技术，以用于对其进行严格设计、操作、测试和检查。
- 开发高级安全体系结构：该研究将组织各种安全组件和服务，为信息与通信系统提供保密性、完整性和可用性。并且，该研究集中关注用于建设最小脆弱性信息与通



信（I&C）基础设施的工具和步骤。所涉及的主题包括公钥基础设施、目录和证书管理、安全组件间的互操作性、新技术的安全执行政策、高级防火墙技术、包转换技术、安全操作系统（用于 Internet 及安全性升级时的补丁和信息自动分布）、安全体系结构的可伸缩性和最优化、远程控制系统中的脆弱性。

- 开发软件补丁的自动分发、安装和跟踪工具：这一项目旨在开发一套软件工具，用于在计算机系统和网络中自动化分发及安装软件补丁，并跟踪补丁的使用，对未曾正确安装或使用补丁的系统进行检测。
- 理解信息保障中的人力因素：该项目讨论信息保障中的人力因素，开发政策和操作建议，以减少相关的基础设施安全风险。预期成果是开发出减缓策略、操作建议以及人事方面的标准。

### （3）基础设施之间的互依赖性

- 互依赖性的确认和特征化：该项目将确认并特征化基础设施之间的互依赖性。特别地，它将研究各种紊乱和错误在多个基础设施间传播的方式。该项目将建立在目前正在进行的一些项目基础之上，以促进对关键基础设施之间的关联、关联的影响以及关联的连带关系的科学理解。
- 开发高级建模和仿真工具：该项目将开发用于国家的各个互联基础设施评估时所需要的系统分析技术、建模和仿真工具以及数据库。国家级的地理信息系统（GIS）基础设施数据库将全面模拟和分析由复杂性和互依赖性而引入的脆弱性。当软件模型无法充分实现模拟时，将采用测试床（这时测试床显得尤为重要）来分析实际效果。
- 后果分析、风险管理、保护和减缓技术：该项目将开发对互操作性相关后果（如对国家安全、经济和社会的影响）进行评估的方法、工具以及风险管理工具。该项目还将确认现有的保护和减缓措施及技术，减少基础设施互联引入的脆弱性。这些措施的作用将从互依赖性的角度加以特征化。新的保护和减缓技术也将进行开发并试验。

### （4）自动化的基础设施控制系统的安全

- 开发高级安全监督控制和数据采集（SCADA）系统：该研究项目将讨论同 SCADA 系统有关的安全问题及脆弱性，从而改善安全状况和协议。另外，还要开发新的体系结构，增强冗余度和可靠性。

### （5）入侵检测和监控

- 开发高级人工智能软件工具用于陷门分析和恶意代码检测：该项目旨在开发高级软件工具和技术，检测并消除软件中的陷门和其他恶意代码。检测对计算机代码的有意但微小的改动是一个难题，这些工具将增强软件产品的完整性，从而减少未来计算机和网络遭到渗透和危害的可能性。
- 开发高级入侵及事件检测和预警技术：该研究将开发在计算机事件、服务瘫痪以及攻击中用于检测、响应和事件恢复的工具和步骤。它的重心将在于衡量标准的开发，以评估误警率、基于策略的入侵检测技术、高速网络上使用的工具和技术、可伸缩的入侵检测系统以及入侵追踪工具。

**关键基础设施保护研究活动时间表：**制定联邦政府关键基础设施保护 R&D 日程，使其成为多年度计划的一部分，并把私营部门的研究考虑进去，从而在一个较快但可控的时间段内将脆弱性减至最小。具体时间表如下：

阶 段	活 动	目标日期
6.1	协调联邦政府关键基础设施保护研发工作，为 2000 年及后续财政年度的预算做准备。确定国家计划执行中需要的研发项目，制定多年度的资金战略，并把第一年的资金要求并入 2001 年度部级预算需求中	已完成 (1998 年 6 月)
6.2	在向私营部门和学术界的咨询下，OSTP（科技政策办公室）将每年更新联邦政府关键基础设施保护研发项目中的优先级	1999 年 9 月，此后继续开展
6.3	召开有工业界、学术界代表和政府专家参加的会议，讨论研发项目的优先级，建立公共-私营机制来协调联邦和私营部门对关键基础设施保护的研发，协调内容 7 中人力和训练方面的工作与资源，建立并支持培训方面研究的发展，使本科生和研究生具有熟练的技术	1999 年 12 月，此后继续开展
6.4	确定国家计划所需的主要研究项目的成功日期	2000 年 1 月
6.5	对创建中央研发联邦基金进行评估，以对横向项目进行支持，确保 2002 年及以后年度预算中公共-私营研究的协调	2001 年 3 月

## 6.2 信息基础设施保护学会（IIIP）

在研发和其他的主要技术领域，不论是私营部门的市场需要驱动还是政府各机构的任务目标，都不可能完全满足国家的要求。信息基础设施保护学会支持关键信息和电信基础设施保护研究和技术的发展，它将弥补这一缺口。

建立这一学会的思想来源于 1998 年 12 月，当时科学技术总统顾问委员会（PCAST）向总统提交了建立一个新学会来解决信息基础设施保护中的研发诸问题的提议。PCAST 的总结中认为，不仅找不到专门致力于基础设施保护知识和公共技术基础开发的技术组织，而且私营部门也没有充分的市场驱动力去完全解决其自身基础设施保护中的研发问题。总统认可了建立学会这一任务的重要性，并责成科技政策委员会（OSTP）和国家安全委员会（NSC）去评审 PCAST 的提议，而且还要向其本人提交推荐意见。这次评审的结论认为，成立一个基础设施保护学会，既有非常巨大的实质需求，也有广泛的私营部门支持。

### （1）运作理念

IIIP 的成功依赖于对多方需求的有效满足：有关的政府机构和部、信息基础设施所有者和所有者、信息技术提供者、学术界、依赖关键基础设施的各公司和共同体。为满足它们的需求，学会将按如下原则构建。

- 学会将只有一个小型的专家工作班子：学会的主要工作是向现有的组织和机构提供资金支持并向其分配任务，这同 DARPA（国防部高级研究计划局）的运行类似。这种运行模型有以下几个好处：
  - 提高了灵活性、质量和效率。学会可以把研究基金拨给最具天分的信息技术专家，不论他们位于工业界、学术界还是政府。而且，通过重新划拨基金，可以迅速调整研究的优先权，而不需要去克服作内部工作所带来的“迟钝”。
  - 避免了“砖块和水泥”式的启动耗费。因为不需要添加新的大型实验室设备。核心工作人员的规模将相对较小，尤其在学会的启动阶段。
- 学会将补充现有的研究，而不是对其破坏：它将同政府、私营部门以及学术界密切合作，协调其信息基础设施保护活动。学会还将为计算机保障基础，如标准和衡量基准、“测试床”规定以及课程开发提供示范和开发支持。这些支持将对联邦和私营部门的 CIO 提供很大帮助，那些在建的服务于州和地方政府及工业界的信息共享和分析中心（ISAC）也将从中受益。

学会将主要关注于为那些在工业和政府现有的项目中没有提及的，有时也不可能通过工业界完成的高科技领域提供基金、促进协调以及将研究进行综合。它将资助高效能的基础研究，也将资助和（或）开展更多的应用性活动，如对美国信息基础设施系统中的脆弱性进行建模并确认以及为信息保障技术提供“测试床”。这些活动中的某些部门也许是敏感性的，因此必须列为机密。学会可能强调对那些广阔的、系统之系统（systems-of-systems）中的脆弱性进行研发和分析，因为这些系统横跨了私营部门和工业界，在合力攻击下会发生大规模严重后果。另外，学会还将对有关各种基础设施之间互依赖性的研究进行资助。

- 通过商务部 NIST 的操作，学会将同工业界和相关的联邦机构结成密切的工作关系。为确保与联邦优先发展项目的协调和相关，学会将向联邦协调委员会做出报告。该委员会的成员包括总统科学顾问、OMB 副主任、NSA 副局长、DAPRA 局长、NIST 会长、NSF 主管以及国家协调员（国家安全委员会）。学会还将寻求来自国家基础设施顾问委员会（NIAC）和部门协调中心的工业界指导。此外，我们呼吁私营企业和各联邦机构也能对各项目进行资助、支持或提供各种实物支援。

### （2）任务和功能

学会的任务和功能将包括（但并不只限于这些）：

- 使工业界从事于学会的顶级战略开发和项目定义。
- 资助、协调、集成那些鲜有提及的科技领域内的研究，将该类研究的成果向各机构适当地转让，使它们能得到应用。
- 为公共-私营合作和信息共享建立双向通路。
- 提供产品评估基准、“测试床”及工具。就这一点来说，学会同 Underwriters Laboratory 公司的角色类似。
- 对学术界提供支持，培训和教育信息保障领域内的研究者及教育者。对该领域内的支持还包括协助课程的开发和提供研究补助等。

### （3）研究领域

在与政府和工业界的密切磋商并在联邦协调委员会的指导下，学会将制定并时常更新其研究日程和研发资源分配。迄今为止，在与各界（私营部门、学术界和政府专家）的磋商中，学会已经指定了很多重要的候选研究领域，包括：

- 物理/计算机/人力接口；
- 入侵监控和响应；
- 恶意代码预防和检测；
- 重建；
- 把基础设施特征化为端到端系统；
- 把信息保障确立为工程原则，包括制定工程原则和测量基准；
- 对端到端系统设计原型并测试；
- 高度复杂、非线性网络的稳健性和韧性；
- 基础设施互依赖性分析，包括建模、仿真以及数据库开发；
- 其他注意力不足的领域（比如 PKI、测试、安全体系结构）。

具体时间表如下：

阶 段	活 动	目标日期
6.6	建立信息基础设施保护学会，对各类研究项目进行资助	2001 年

## 内容 7：建立由高技术计算机科学和信息安全人员组成的核心——联邦计算机服务（FCS）培训和教育活动

受过高度训练的信息系统安全专家是联邦政府信息系统保护项目的基础。但不幸的是，在整个联邦政府、学术界以及私营部门，这些信息安全专家严重短缺。我们需要足够多的联邦高技术信息系统安全专家，为此就要有新的项目——联邦计算机服务（FCS）培训和教育活动。这一活动由 5 个主要部分组成，将做到：确定 IT 人员短缺状况；开展新的人员补充、教育和人员保持工作；向联邦业务中的专职信息安全专家进行不断的培训和认证；向所有的联邦工作人员灌输信息安全意识。联邦政府还将同私营部门合作，包括工业和学术界的机构，以决定怎样最好地扶植教员的发展，使他们能够培训出满足我们的信息安全需要的专家来。

不同的渠道都曾经反馈过信息系统人员的短缺问题。1997 年审计总署（GAO）的一篇报告中记述了联邦政府内的信息系统人员短缺情况，报告中总结道：联邦政府“缺少具有管理控制技术知识的人员”。据估计，在整个国家的范围内，我们的经济将在未来 10 年间需要大概 130 万新 IT 人员。但令人吃惊的是，从 1985 年至 1996 年，每年毕业的计算机科学学位获得者的数目竟下降了差不多 30%，这一趋势直到最近才有所减缓。我们要通过综合性的工作来训练和教育我们的 IT 雇员，并向所有的联邦提供基本的安全意识培训，这是亟待完成的。

在发展 FCS 活动的过程中，我们可以利用现有的联邦教育、培训和意识培养项目。在教育方面，国家安全局（NSA）的项目为：指定某些大学作为信息保障教育中的优秀学术中心，指定过程中参照的是国家安全电信和信息系统安全委员会（NSTISSC）培训标准中确立的原则。另外，GSA 已经发起了一个 CIO University（首席信息官大学）活动，旨在提高高级联邦 IT 雇员的知识和技能。在培训方面，国防信息系统局（DISA）已经开发了一系列信息保障培训工具，供国防部内使用，并随后对这些工具作了“量体裁衣”，使其也能在其他联邦部门中得到应用。其他一些部局也就其自身需求对这些工具做了开发和发展。国防部的 DIAP（国防信息保障项目）业已制定了一个子项目，基于常规培训、岗位培训以及工作经验对国防部的信息保障工作人员进行认证。NSTISSC 的教育、培训、意识培养焦点组在国家信息保障培训标准方面的工作也是一个值得借鉴的重要成果。在意识培养方面，CIO 委员会已经专门责成两个机构研究这一问题。此外，我们还将向联邦信息系统安全教育者协会（FISSEA）的专家和联邦计算机安全项目管理者论坛寻求帮助。NIST 在 1998 年 4 月对信息安全教育问题发起了一次出色的跨机构评审，其报告《信息技术安全培训要求：基于角色和表现的模型》（NIST SP 800-16）是一个信息安全培训概念性的框架。该报告清楚地展示了开展意识培养项目、实施信息安全培训以及对 IT 雇员进行教育的需要。FCS 活动的很大一部分都是建立在这篇报告的框架基础之上的。

### 7.1 政府范围内的信息技术职位研究

开展 FCS 活动的第一步就是完成 OPM（人事管理办公室）信息技术职位研究。该研究将更好地评估联邦政府内的各类 IT 职位（比如网络管理员、安全专家等），并可以更加准确

地定义各 IT 职位的信息安全能力要求。这对于确定众说纷纭的政府机构中 IT 安全人员的短缺情况非常重要。另外，信息技术职位研究还将有助于确定联邦政府 IT 人员的培训需求。

人事管理办公室将评审政府对 IT 职位管理的全面办法，并将制定一个基于能力的工作轮廓试点，以取代当前用于选择 IT 人员的最小资格要求。OPM 还将研究出一组新类型的 IT 职位，并为这些职位制定专门的名称，从而取代过时的 IT 职位分类标准。OPM 将与感兴趣的机构联合制定一项提议，用以解决相关的权限和拨款问题，以确保政府具有招募、训练和供养联邦安全保障人员的能力。职位研究的结果还将用于促进 SFS（见 7.3 节）和中学项目（见 7.4 节）候选人的招募、选择和培训。IT 职位研究得来的数据将用于 IT 工资系统的评审和设计。

## 7.2 信息技术优秀中心（CITE）

CITE 将为联邦 IT 安全雇员、联邦承包商以及 FCS 候选人提供高级的信息安全培训和认证。中心将提供下述功能：

- 为联邦雇员 IT 职位专门化提供基于网络的和（或）课堂的技术培训；
- 在 FCS 职业教育项目中向各学院和高校学生提供培训和认证；
- 更新、加强和维护已达到认证要求的那些联邦雇员及 FCS 候选人的技术水平。

最初，CITE 的发展集中于使用现有的培训标准向系统管理员和信息系统安全官（ISSO）提供培训。这些现有标准中包括那些正被 NSTISSC、CISSP（信息系统安全专家认证）以及其他国内外团体采用的标准。中心将来的扩展将集中于对系统认证员、风险管理、计算机科学家、计算机工程师、计算机程序员和系统分析员进行培训。联邦雇员和联邦 FCS 候选人采用的认证和再认证过程将以其他过程为模型，包括：正在发展的国防部关键 IA（信息保障）人员认证过程；CISSP 开发的认证过程；其他国际国内认证团体开发的认证过程。如果雇员参加了认证项目且认证项目达到或超出了 CITE 制定的最低标准，那么他所取得的认证我们将予以承认。可以通过中央人事数据档案（CPDF）检索已通过认证的专家。

CITE 的发展离不开对现有设备、课程、教职员资源的利用。**任何能够成功证明其有能力向联邦雇员提供知识和技能、向 FCS 候选人培训认证时要求的专业技术能力的组织，均可以纳入 CITE 网络中。**这种组织可以是学院和大学、政府培训基地，或者是基于私营部门的技术培训中心。认证过程将参照发展中的 NSTISSC 课程软件和课程认证过程。我们将依靠 CIO 委员会、NIST 安全培训报告和 OPM 职位研究来提供专门指导方针，并制定培训和认证的标准。我们的目标是建立一个全国范围内的 CITE 网络，向联邦 IT 雇员提供标准化的培训，使他们达到 OPM 要求的技术水平。

国防部的工作是很值得利用的。目前人们正在评估其新开发的“高级分布式学习网络”，它可以向国防部的各工作岗位提供基于互联网和（或）基于计算机的信息保障知识和技能培训。该网络将利用已开发出来的 IT 安全雇员培训产品或国防信息系统局（DISA）正在开发的产品进行人员培训。国防部已经表达了其愿意同联邦民事机构合作来扩展这一网络的意向，以使该网络覆盖整个联邦范围内各机构的 IT 岗位。“高级分布式学习网络”知识和技能培训的方法多种多样，包括基于教室、基于计算机、基于互联网和远程教育。

### 7.3 SFS（服务奖学金）项目

教育和雇用新的联邦 IT 雇员及安全管理人员的主要办法是面向大学学生的 SFS（服务奖学金）项目。在该项目中，政府将资助研究生或本科生的学习，使他们达到信息保障标准的要求，作为偿还，这些学生要事先同意学成后服务于联邦政府。

SFS 项目将为硕士（M.S.）或博士（Ph.D.）候选人提供两年的奖学金；向在一个备案认可（accredited）<sup>①</sup>信息安全项目中攻读理学士（B.S.）学位的大学三、四年级的有前途的学生提供为期两年的奖学金；向在一个经批准的两年期 IT 项目中攻读 A.S.或 A.A.<sup>②</sup>学位的 IT 安全雇员提供为期两年的奖学金。

SFS 项目将向学生提供学费和适度的生活津贴，除此之外还有很多其他福利。学生将参加各联邦机构的暑期工作和实习项目，还可以参加政府实验室的工作。对这些学生来说，他们得到的经验将为他们在联邦部门就职提供指南，并且可以使他们更加清楚在学业阶段他们应该发展哪些技术。对联邦机构来说，学生的暑期工作将对正在进行的 IT 安全工作帮助颇大，并且使他们得以对 SFS 项目中的各参与学校的表现做出评估。暑期工作和实习还可以同 CITE 中的联邦 IT 安全培训项目及后续的认证结合在一起，使学生在 SFS 项目结束后能快速并高效地投入到联邦服务中。SFS 学生还将参加一些定期举行的会议，包括国家信息系统安全教育讨论会等，以增加他们的学术和技术经验。暑期工作和实习项目的管理将同 7.4 节中讨论的高中活动保持协作。

要确保 SFS 的成功，关键一环是对项目中开设信息安全课程的参与方大学和学院进行确定和备案。目前，在美国大学中只有有限的几个信息安全研究生培养计划，这造成了在信息安全领域既缺少教授也缺少活跃的学生。在本科生课程中，情况同样如此严重。这反映了计算机学位获得者的数目总得来说在走下坡路这一危机——从 1985 年到 1996 年，每年毕业的计算机学位获得者的数目从 50 000 下降到了 36 000。联邦政府必须同学术机构和工业界合作，共同遏止并改变这种人才短缺的状况。

在信息保障项目的开发方面，政府还有类似几个与大学建立的合作关系，包括 NSA 的国家 INFOSEC 教育和培训项目（NIETP）。NIETP 为 INFOSEC 课程的开发提供了标准和指导方针，帮助建立了 INFORSEC 教育基础设施，并确定了一批符合标准的学校，将它们指定为信息保障教育优秀学术中心。在 NIETP 项目的第二年，还将考虑批准同样数目的一批大学进入。我们可以同 NIETP 和优秀学术中心在信息保障教育项目中密切合作，为 SFS 活动确定学校。

已经有了相应的备案认可标准，用以确定和认可信息保障领域的领头羊大学，但必须有范围更广的联邦实体对其承认（NSA 的信息保障教育优秀中心项目的标准是基于 NSTISSC 培训标准制定的，后者得到了 21 个联邦部门的承认）。各中心必须有能力传授尖端的 IT 安全技术知识。当前的和未来的中心必须要得到评估，确定它们是否有能力为信息保障教员的发展和进修提供资源。这些中心的功能将包括：

➤ 传授经联邦认证的课程；

① 认可备案是指由全国承认的有关鉴定机构对一个学校、教育单位和（或）其中某个项目的非官方性质的认可。一个学校和教育单位是否备案关系到学生攻读学位期间一个学校（或单位）的学分能否得到另一个学校（或单位）的承认，也是学生获得专业证书或许可证的先决条件。——译者注

② A.S.：（associate in science）准理学士；A.A.：（associate in arts）准文学士是指由社区学院（Community College）或专科学校院（Junior College）在学生修完两年普通课程后授予的学位。学习两年制课程的学生一般准备将来从事职业性质的或技术性质的工作。——译者注

- 传授初级和高级的教学技巧；
- 辅以合适的实验室演习、电视节目、远程教育以及公共项目，对联邦认证的课程进行补充。

必须要建立 3~5 年的评估标准，以促进并确保其“优秀”的普遍性。该项目还需要有内建的激励机制（即优先获得津贴等），这可能会要求联邦在人员“采购”方法上发生些变化。在国家信息系统安全教育讨论会上，所有这些标准都将同更广泛的工业和学术界进行讨论。

CIO 委员会和总务管理局（GSA）已经为高级执行官开发了一个补充式的教育项目——CIO University（CIO 大学）。这个 CIO 大学是由四个大学组成的一个虚拟教育协会。它可以提供研究生水平的课程教育，直接针对 CIO 委员会所采纳的执行官核心能力要求。CIO 大学的目的是通过提高高级 IT 执行官们的技术，改善政府的信息系统管理水平。项目从跨时 8 星期到 3 学期不等，最终要使参加者获得 CIO 证书，并且如果可能的话，可获得理学硕士（M.S.）学位，具体要根据他所选择的学校的课程。

对 SFS 合作大学的认证还将有助于使各大学采取更加一致和更加快速的行动来促进 IT 教员和信息安全项目的发展，使在信息安全领域内接受有效教育的本科生和研究生的数目得到增加。这些研究生中，很多人将进入政府和工业界，还有一些将留在学术项目中，以满足日益增长的国家需求。政府同学术界的合作关系还包括，联邦将在 SFS 项目的参与大学中帮助建设教员职位和 IT 安全实验室。显然，可以利用 NIETP 和 CIO 大学等已有的项目来确定可能的参与方大学。

#### 7.4 中小学推广项目

IT 领域内一个明显的趋势是，年轻一代有了参与世界并在这个世界中竞争的能力。这促使我们着手开发一个中小学推广项目。该项目的主要目的是：

- 提高初中学生和老师的对 IT 安全和联邦计算机服务的**认识**；
- 就信息安全和联邦计算机教育及工作机会向中学学生和老进行**宣传教育**；
- **确定**中学里那些具有天分、并愿意在大学阶段学习信息安全的学生。

中学推广项目有很多内容，包括：面向老师和学生发起一系列会议、夏令营、暑期工作项目和实习活动，鼓励他们参与到信息安全保护课程中来；确定并招募一些有前途的学生，使他们中学毕业后立即到联邦政府 IT 岗位上工作；招募未来的 SFS 项目候选人。夏令营可以同联邦政府的培训项目（CITE）整合到一起，使参加者作为联邦政府将来可能的雇员，得到系统管理员认证，增加他们对政府工作和标准的认识，提高他们对联邦机构的评价。

就信息安全诸问题对小学学生和老进行教育既有学术益处（即个人意识、隐私保护、工作、研究技巧），也有很多道德益处（即学校安全、个人责任）。教育部已经开始同学术界和私营工业密切合作，制定并推广有关对学生进行计算机安全责任教育的标准和出版物。比如，教育部在 1998 年同国际教育技术学会及各种各样的政府和民间组织进行了合作，以共同发展 NETS（国家教育和技术标准）项目。这一项目为早期 IT 教育提供了 4 类标准。另外，为了发展小学教育项目，教育部还出版了一本综合性的初级读物《保护你的技术：电子教育信息的安全保护操作方针》<sup>①</sup>。我们将继续评估各类小学计算机教育项目，并考虑建设一个联邦互网站，以支持课程开发和传播。

<sup>①</sup> 该文主要讲述怎样有效保护电子教育中的技术和设备，全文见于 <http://nces.ed.gov/pubs98/98297.pdf>。——译者注

## 7.5 提高联邦雇员的 IT 安全意识

PDD63 以及关键基础设施保护总统委员会均要求联邦政府在 IT 行动方面成为私营部门的榜样。为了能够有效对付针对联邦信息系统的威胁，有必要确保所有负责确定计算机威胁并采取合适行动的联邦雇员都对各种威胁了如指掌，而且知道应该怎么做。本节中的“意识培养”项目的目标就是确保所有的联邦雇员都知晓计算机入侵给联邦系统带来的威胁，使他们能够标识这类事件，并且知道应该采取哪些步骤来响应事件。我们的策略是，开发并执行一个计算机基础知识普及项目，包括发布简报以及开展那些能够被每一个联邦机构视其目的而采纳的相关活动（如借助 CD-ROM、录影带、演习、研讨会、展示会等）。还将制定“意识培训确认录”，并提供给各联邦机构使用。这些“确认录”将会记录下各机构定期开展计算机意识培养活动的情况。

意识培养项目开展过程中将会与 CITE 紧密协调，使用 CITE 的基础设施来开发并发布各种 IT 安全意识培养产品。像 IT 安全培训产品一样，这些产品可以基于互联网或 CD-ROM，也可以是录影带或简报资料等。国防信息系统安全局（DISA）已经开发出了几个有益的“INFOSEC 意识培养”CD-ROM，可以用于国防部，经适度改动后的产品会在非国防机构中使用。对这些已有的成果，我们将会权衡利用。要仔细检查 IT 意识培养和计算机基础教育工具，以确保他们按要求做到了定期更新。

**建立由高技术计算机科学和信息安全人员组成的核心时间表：**要建立各种项目以在联邦政府内拥有并维持受过高度训练的信息技术安全专家。为此，我们需要：

- 完成政府范围内的综合性 IT 职位研究，确定所有的 IT 安全职位以及这些职位的能力要求。
- 针对信息系统安全中的联邦信息技术雇员，建立培训和认证项目。
- 建立服务奖学金（SFS）项目，向信息系统安全学科中的学生提供奖学金（在备案学校），条件是他们将来要到政府部门服务。SFS 还将发展信息安全学科的教员，并进行信息安全课程的开发。
- 针对中小学学生和老师，设计推广和意识培养项目，从而鼓励他们在将来成为联邦 IT 雇员，该项目还将对所有的学生施以计算机安全道德教育。
- 开发并执行联邦 INFOSEC 意识培养课程。

具体时间表如下：

阶 段	活 动	目标日期
7.1	开始大学的推广工作，以推动服务奖学金（SFS）项目的发展。对 SFS 候选人进行认证，建立专题讨论会以招募可能的候选人。如果需要，为任何其他权威项目制定提议	2000 年 1 月
7.2	对联邦范围内信息系统安全培训和教育项目进行完整的评审，确定现有的培训和教育项目，找出任何差距或冗余	2000 年 3 月
7.3	为大学申请并被选入 SFS 项目制定标准、备案要求和指导方针	2000 年 4 月
7.4	利用国防部和私营部门的模型，开发联邦 IT 安全雇员认证项目，用于系统管理员和各 ISSO（信息系统安全官）；开发培训项目，用于满足这些认证目标的需求	2000 年 5 月
7.5	开发并传播联邦岗位 INFOSEC（信息安全）意识培养课程。各 CITE 中，其中一个将负责这些项目，预先审查和更新其内容	2000 年 5 月
7.6	制定指定 CITE 时的标准	2000 年 6 月



续表

阶 段	活 动	目标日期
7.7	设计和执行中小学推广计划，包括各种会议、暑期工作和实习	2000 年 7 月
7.8	任命参与第一年 SFS 项目的一批大学	2000 年夏
7.9	在联邦政府内完成由 OPM（人事管理办公室）所领导的对信息系统安全职业需要进行的研究。这将为联邦 IT 岗位的人员征募、推广、选择、工资偿付和能力发展提供可靠的数据	2000 年夏
7.10	为未来的 SFS 教职员开展一个试验性的信息系统培训项目。这将成为我们的教职员发展项目的前导	2000 年夏
7.11	为 2001 年开始的第一年 SFS 项目招募研究生和本科生，以后每年招 300 个学生	2000 年秋
7.12	确定、指派各 CITE，并为其提供资源。中心将为联邦 IT 雇员开发、提供高质量的信息系统安全培训和认证；还向 SFS 和暑期工作项目中的中学生提供技术认证和训练项目	2000 年 10 月
7.13	第一批 SFS 项目学生开始学习	2001 年 1 月
7.14	SFS 计划的第一批研究生进入联邦 IT 工作岗位	2002 年 5 月

## 内容 8：推广和意识培养

### 8.1 关键基础设施安全中的合作组织（PCIS）

要确保关键信息系统的安全，避免其发生严重故障或受到外部攻击，就要在个体公民和私营商业、州和地方政府、联邦政府之间建立前所未有的合作关系。为了最终的胜利，这种合作关系必须建立在对威胁和响应的公共认识和理解的基础上。

**关键基础设施安全合作组织**将是工业界和政府之间的一个国家级的合作工作，主要聚焦于工业界和政府互相协作的迫切需求，以确保国家基础设施的关键服务的正常运行。

这一合作组织将得到政府最高层和美国各大公司首脑的支持，这是其鲜明特点。它将为广泛的意识培养活动建立框架和保护伞。

为此，合作组织将发起有工业界和政府部门执行官参加的一系列的讨论会、集会和工作组，为达到下述目标而努力：

- 促进关键基础设施所有者和所有者、风险管理团体、普通商业团体、州和地方政府以及全美国人对信息安全的意识和理解。
- 促进工业界在未来向国家计划做出贡献。
- 确定并解决大家所共同关心的问题，包括但不限于信息共享安排、法律和法规改革、标准和最佳实践措施、教育和培训以及研发活动。

合作组织的发展将基于：开放和自愿的成员资格；双边信任；经常性的交流；对于各参与方的价值体系、期望、需求、关心和目的的充分理解；对取得清晰、集中、得到良好定义的目标的信念。

CIAO 将对联邦政府在合作组织中的参与活动进行协调。为了支持合作组织的发展和各方参与，它还将同各行业的联邦领导机构及这些机构各自对应的私营部门一起工作，制定使合作组织更加有效的战略和计划，并提供项目指导和各种材料。

8.2 “计算机公民”活动

美国信息技术协会（ITAA）和司法部开展了一个补充式的国家运动，针对其他公共-私营合作活动来给予教育和意识培养，并提供必要的资源。计算机公民的活动将：

- 对儿童、年轻人以及更广泛的用户团体进行关键信息保护方面的基础教育，并使大家知道合法在线活动的范围和限制。活动的第一步将集中于对 K~8 年级的儿童用户进行教育，向他们解释计算机使用道德的重要性。
- 出版计算机和网络安全字典，使公共和私营部门在保护其信息资产时能够迅速找到所需的计算机安全资源。
- 在工业界和联邦政府之间建立正式的人才交流项目，推动教育和意识培养活动的发展，促进产品开发，并创造进一步的合作机会。

美国的决策部门必须理解并采取行动来保护我们的关键系统，同样，所有美国人都必须理解在 Internet 和其他信息系统中“遵纪守法、行为适当”的重要性。

8.3 联邦雇员的培训

联邦政府要想成为信息系统安全的模范，那么其所有的雇员都必须对此目标做到心领神会。为此，我们要做的第一步重要的事情就是，确保计算机安全和规范的信息系统操作方面的信息和内容能被数以百万计的联邦公务员所知晓，并且能够被管理者所响应。

所有联邦雇员每年都要接受很多内容的教育，这些内容对国计民生非常重要。比如，对雇员岗位上道德规范的重要性进行教育等。同样，通过经常性的培训活动，我们将努力确保所有的联邦公务员都懂得信息系统安全的需求，领会确保联邦和国家系统不受损害的那些简单但必要的步骤。

推广和意识培养活动时间表如下：

阶 段	活 动	目标日期
8.1	通过创建计算机公民项目，对美国儿童施以使用计算机系统时合适行为和道德方面的教育	已完成 (1999 年 5 月)
8.2	通过创建公共-私营关键基础设施安全合作组织项目，提高各公司及政府对关键信息系统和计算机网络所受威胁的认识	2000 年 2 月
8.3	向所有可以接触敏感信息系统的联邦政府人员提供命令性的计算机安全意识简报。这种简报在他们一接触其业务时就要提供，并且以后至少每两年提供一次	2000 年 3 月

内容 9：法律和立法分析及改革

在联邦政府努力保障其关键基础设施的工作中，还应对法律和政策进行仔细地评审。4 年多来，政府已经系统地调查了法律改革方面的诸类事项。现在，法律改革过程中的 7 个原则已浮出水面。

第一，法律改革必须经过集中的讨论并有各方的参与。关键基础设施保障政策不但涉及很多私营部门，还横贯了各个政治和地域边界。

因此，任何成功的法律改革工作必须得到下列实体的参与：

- 广泛的行政机构；
- 作为行政部门的一部分的各个组织，如 CIO 委员会、廉政和效率总统委员会（PCIE）等；
- 国会，包括其下属机构，比如美国审计总署等；

- 联邦和各州的法官、公诉人以及美国判决委员会；
- 各州和地方的法律制定者、条例制定者、第一时间响应人员；
- 学术界，包括智囊团和研究中心；
- 私营工业，包括贸易和职业协会。

第二，政府无意创建并实施范围广阔的法律新体系。针对这篇国家计划中讨论的很多关键基础设施保护要求，国会和行政部门早已经创建了必要的相关法律。

第三，政府在创建新的法律和政治结构时，将以现有的政策和制度为基础。比如，银行管理者已经转变了现有的报告机制，使其能涵盖计算机入侵，而以前，可疑活动报告只涉及物理威胁，对有关计算机的威胁谈之甚少。最近，货币审计师办公室发布的公告唤起了大家对金融服务工业中由计算机恐怖主义制造的威胁和脆弱性的重视和意识。其他机构也正协调其已有的法律项目，使计算机和物理方面的事项都能包含进去。

第四，当需要新法律时，政府的重心在于那些能够减少关键基础设施保障阻碍的解决方案，而不会增加政府和工业的管理负担。比如，现有的法律可能造成了政府和工业界的信息共享变得很复杂，对此的法律调整应该是想办法鼓励更多的信息共享，而不是增加新的管理层或使政府现有的职能复杂化。

第五，法律改革策略必须为技术变革和发展留下余地。事实上，技术进步可能超过了国会法令和各机构条例制定的步伐。为此，法律制定者们有责任懂技术，尤其是技术对现有法律的冲击。除非政府官员们负担起了这种责任，并且同专家、系统管理员以及其他对我们的计算机网络和关键系统最为精通的人们实现了合作，否则关键基础设施政策的制定将是一个痛苦且难捱的过程。

第六，法律改革必须建立在对关键基础设施保障领域内的专门研究和调查结果的基础上。

本届政府从 1995 年开始就认真研究基础设施保障，并委任了关键基础设施工作组（CIWG）。CIWG 由司法部副部长任主席，为解决基础设施威胁研讨和辩论了很多可选的长期战略。重要的是，CIWG 还建立了一套基于“基础设施”和物理、计算机威胁的方法论，总统随后将其并入了 13010 执行令。在 13010 执行令下，成立了关键基础设施保护总统委员会（PCCIP）。

PCCIP 对法律改革选项曾研究了 15 个月之久。这一广泛的综合性研究包括向众多政府实体和代理人的推广，其中有执法部门、大律师、首席信息官和国防部门。分别代表政府和私营部门的委员们就法律方法论和各类法律主题进行了广泛的调查。最终，PCCIP 的研究结果和结论冠以《法律基础》出版，该书阐述了推进法律改革时要用到的进一步的知识和经验。从 1998 年 5 月开始，国家协调员已经组织了一次对各关键基础设施建议书的评审，这也是政府在进行法律改革时应考虑到的。

第七，法律改革必须确认并支持全面的隐私权和公民自由要求。为此，政府要清醒地认识到：关键基础设施保障政策一定要继续提高隐私权以及其他的宪法所赋予公民的权力，保护美国商业的私有产权。本篇国家计划专门以独立的一章来详细讨论公民自由。

### 9.1 在计划的执行前，评审是必要的

在这里，政府将评审现有的法律条款以及联邦信息保障计划的执行要求。司法部将担负领导作用，协调法律改革的发展。评审将包括如下要素。

### 9.1.1 使联邦政府完成其保护关键基础设施的工作，并使其成为领导典范

- 采购改革：在合适的地方，联邦政府应当把基础设施保障考虑同基本采购和未来采购结合起来。采购政策和条例中的疏漏或不足都有可能危害到基础设施保障的目标。

法律改革将检查采购政策和条例是否考虑了基础设施保障目标；研究这些目标是如何在其中得到容纳的；还要对未来采购政策和条例的修订做出提议。法律，包括 1995 年颁布的《减少文书工作法》以及 1996 年颁布的《Clinger-Cohen 法》要求各机构关注信息技术的采购和信息资源的管理。任何法律改革都应该建立在这些基础之上。

- 标准和认证：在信息安全标准的遵循方面，联邦政府应该成为私营部门的榜样。诸类标准为政府发起的各认证项目提供了基础，使它们能够符合与安全相关的那些目标。不能要求官僚机构去监督政府发起的认证项目的实施和执行，这些项目要有各种激励机制来鼓励私营部门的参与。
- 工作绩效评定：《政府工作绩效和结果法》（GPRA）要求在预算过程中，OMB（管理和预算办公室）要对联邦机构 5 年期战略计划作审查，还要针对主要职能运行时的表现评定做出审查。《Clinger-Cohen 法》要求对工作表现的评定应该同信息技术的使用结合起来。但所要求的工作表现评定不只包括信息安全。

在各机构的 GPRA 战略计划和工作表现评定框架中，应该鼓励它们把其承担的基础设施保障职能包括进去。已有人对《Clinger-Cohen 法》做出了修正提议（该提议即将被讨论），要求各机构首席信息官（CIO）为其信息系统的安全进行性能评定，并应在法律需要的时候将评定结果提交给 OMB（管理和预算办公室）。对一些有选择的系统来说，如果定量评定结果的提交会危害到国家安全，那么那些国家安全单元可以免于提交这种工作表现评定。法律改革工作应该有政府审计总署的参与，因为该机构已认真研究了上述问题并提交了各类矫正性建议。

- 入侵检测：开发具有评估、报警、隔离事件以及重建重要信息等功能的系统是我们这个计划长期成功的基础。入侵检测系统（IDS）的开发引发了各类的法律和政策问题，所有这些问题都是政府所必须认真研究的。

作为跨机构法律评审过程的一部分，IDS 的这些法律和政策问题主要由司法部研究。主要的法律议题包括：

- 政府在 IDS 产品开发中涉入的范围和程度；
- 当数据库的内容没有得到充分保护时，联邦政府所应承担的责任；
- 监控、访问、使用和传播有关信息的步骤；
- 同 IDS 有关的隐私和公民自由综合性问题。

#### 总检查长（Inspectors General）

总检查长的未来角色

基础设施保护中的计算机入侵事件、审计、执法

自 1978 年以来，联邦机构检查长就在制定、审计和强化联邦政府管理及安全措施方

面扮演着重要的角色。法律改革和本篇国家计划的执行将同他们的角色、责任以及积极参与密切相关。

当前，PCIE（廉政和效率总统委员会）以及 ECIE（廉政和效率经济委员会）它们是根据 1992 年 12805 号执行令《联邦项目中的廉政和效率》成立的<sup>①</sup>正在为检查长积极参与关键基础设施保护过程而制定参照模型。根据 PCIE，检查长的总目标中要包括针对如下活动的开展进行充分性检查：

- 机构在基于计算机的关键基础设施保护中的计划制定和评估活动；
- 机构在基于计算机的关键基础设施保护中的执行活动；
- 机构在非计算机关键基础设施保护中的计划制定和评估活动；
- 机构在非计算机关键基础设施保护中的执行活动。

尤其是，检查长们已经声明，他们正评审各机构在如下风险管理领域内的活动充分性：风险减缓、应急管理、跨机构协调、资源和组织需求以及人才招聘、教育和意识培养。

### 9.1.2 确保有效的政府-工业界关系能够建立

- 信息共享中的法律障碍：基础设施保障中信息共享机制的成功将在很大程度上依赖于可信环境的建立，它应促进各方——政府和私营部门在自愿的基础上参与敏感信息的共享。然而，目前存在的一些法律障碍却可能阻碍或不利于各方的参与。这包括对某些潜在责任（如反托拉斯、侵权等）的担忧、国家安全考虑、信息的密级、强迫向公众作公开的那些法律程序、私有财产和商业秘密的保护考虑等。

《信息自由法》和其他一些相关的法律决定了联邦政府拥有和控制的信息要向公众开放这一规定。但是信息共享机制中的某些参与者可能会要求一旦他们提供的敏感信息被联邦政府共享，这些信息能得到某种程度的保密。同时联邦机构也可能要求在保护基础设施时他们发现和共享的那些敏感的脆弱性信息也能得到某种程度的保护，不至于向公众全部透露。政府的法律评审将关注与此相关的法律和处理步骤的改革，以有效地克服上述以及其他类似的障碍。

### 9.1.3 减少不必要的法律障碍，促进足够数量的信息技术专家的招募和留任，以确保联邦政府自身关键系统的安全

政府将支持 OPM（人事管理办公室）对此问题的研究。法律改革可能需要针对各种各样的解决方案进行跨机构讨论。

### 9.1.4 联邦制诸事项也决定了要对合作框架进行评审

关键基础设施保障政策和项目中涉及很多同联邦制有关的事项。本届政府始终如一地把关键基础设施保障看作一种合作关系——不论是公共部门还是私营部门之间、不同的政府机构之间，还是州和联邦政府之间。很多复杂的司法问题希望在这一合作框架内得到解决，但是还有很多则很可能有待于进一步研究。

- 州法律对于关键基础设施保障的冲击：根据 1999 年 8 月 5 日发布的行政令 13132《联邦制》中阐述的原则和政策，本届政府将确定在实现本篇国家计划目标的过程中各州法律可能会互相冲击（正面以及负面）的领域。正如本节所谈到的，关键基础设施保障必须包括广泛的参与者和广泛的讨论。与来自各组织，包括国家律师协会、国家州长协会、州政府委员会、美国市长讨论会、国家县长协会、州议会、州

<sup>①</sup> 关于 PCIE 和 ECIE 的资料见网站 [www.ignet.gov](http://www.ignet.gov)。——译者注

判决委员会以及应急管理协会的代表的对话将有助于理想法令的产生。还要有更多的州和地方实体参与到支持并发展关键基础设施保障的法律改革中来。

#### 9.1.5 权限：角色、责任的冲突、重叠和分类

跨机构的评审过程将包括对机构权限问题的综合性研究。各机构的角色和责任是其内在的特征，同时也是国会的宪章以及总统的《机构重组法》所规定的。虽然国会和行政部门为不同机构定义了各自的法律和政策制定功能，然而关键基础设施保障任务却向其中增加了一些与现有模式不太吻合的内容。

本小节中法律改革的讨论包括权限重叠、可能冲突的解决以及政策执行中的豁口等。一些特别例子有：

- 计算机入侵事件和检察官的角色及责任；
- 《计算机安全法》的有效、综合执行；
- 在计算机入侵和相关事件调查中，国防部、情报机构、执法机构和民事机构的合作；
- 安全政策委员会与国家安全电信和信息系统安全委员会（NSTISSC）的任务重叠；
- 各种信息系统中国家安全和应急战备电信法令的执行。

#### 9.1.6 应急响应计划和机制

关键基础设施保障中的紧急事件可能会引发现有的应急响应计划和机制的改革。国会、总统以及行政部门已经制定了很多应急响应法令来支持这些关键基础设施应急响应机制。

跨机构的评审过程将考虑现有的法令和计划如何能对关键基础设施诸问题进行支持。当出现空白的时候，评审过程将对现有法令和计划的修订做出建议。州和联邦政府的计划制定机制应该得到评审，以确保已经采取了各种合适的机制来预防出现工作重复和混乱。一些例子包括：

- 联邦响应计划&应急支持功能（用于所有的紧急事件）；
- 非战时应急电信支持国家计划；
- FBI 应急计划；
- 化学/生物恐怖主义联邦响应中的 HHS 健康和医疗支持计划；
- 联邦电波导航计划（GPS，全球定位系统）；
- 国家应急计划（石油矿井）；
- 联邦放射性应急响应计划（放射性紧急事件）；
- 各州和私营部门的计划。

#### 9.1.7 其他法律改革

政府将认真监督跨机构评审过程对其他有必要研究并可能进行法律改革的领域所进行的讨论。

### C. 国防部（DoD）基础设施保障计划

国防部的很多国内外资产对其战备和军事行动意义非凡，为此它将确保这些资产的可用性、完整性、生存力以及充分性。国防部的战略目标是，确保它对国内外基础设施的依赖性不会反过来削弱其执行国防和全球军事行动的能力。

在联邦各部中，没有哪个地方像国防部（DoD）这样对信息技术（IT）的依赖性如此明显。通过对 IT 的应用，国防部可以提供更加可靠的情报，使指挥和控制系统得到根本的改善，

使其业务操作做到标准化，IT 还可以使其得以开发出威力更加强大的武器系统。因其保家卫国的任务性质，DoD 在保护国家的基础设施、抵御威胁国家安全的计算机攻击或其他事件的工作中要首当其冲。

CIP（关键基础设施保护）将确保国防部的任务及职能所依赖的那些基础设施能够有效地运行。CIP 将着眼于我们如何满足国防任务要求（如所需的设施、装备、信息系统、网络、人事及合约等）、判断我们的关键性资产、确定相关的脆弱性、明确互依赖性以及对关键资产采取保护性措施。CIP 用防御而非攻击性的眼光来看待世界。虽然国防部长久以来就注意保护其国内外的设施（如基地和装备等），但现在要研究这些设施之间如何相互依赖以及它们对私营部门服务的依赖情况，因此我们看问题的角度要与以前稍有不同。

### 制定保护计划

国防基础设施保障计划由 3 个不同部分组成，它提供了一个有效的框架，可以供联邦政府和私营部门在制定其计划或框架时参考。国防部已经创建了用于确定和矫正脆弱性的组织结构，开发并配置了入侵检测系统，发起了很多重要的创新性研发活动。

国防部的计划既包含了物理方面的 CIP，也包括了计算机方面的 CIP，它是后续行动的基础。在后续行动中，我们将解决全面的国防行动的系列问题；明确并理解关键基础设施的互依赖性；采用并整合传统的安全条例及信息保障手段；平衡利用最近的以及现行的国防部活动来满足该部和国家的基础设施以及信息保障所面临的当前及未来的挑战；并建立起必要的 DoD-私营部门合作关系。

国防部将通过如下 6 项活动来实现其关键基础设施保护的目标：

- 分析和评估；
- 矫正；
- 迹象发现和预警；
- 事件减缓；
- 响应；
- 重建。

重要应用：物理资产以及基于信息的各种活动均可以通过以上 6 项措施得到保护。

### 国防基础设施的范围

在当今全球化的信息环境中，IT 革命已经深入到了美国国防任务的每个角落。

- 我们在阵地上的士兵将可以立刻向其长官通报他的确切位置、状况甚至心跳频率，此即完全的“战场空间识别”<sup>①</sup>。
- 我们正使用 Internet 来满足我们的广泛需求——从旅行付款到卫星通信以及电子商务。

国防基础设施（DI）是一种复杂的、互依赖的分散式网络，由各种系统、服务、人员和操作组成，包括私营部门以及其他的政府部门的一部分职能，它横跨了国防部的各组织边界，为国防部的各种需要提供实物和服务。DI 可以分为 11 个下属单位（如财政、后勤、运输和人事等），这些部门拥有着各类资产，有的比较简单（如一件设备或地理位置集中的一套信息

<sup>①</sup> 英文为 battlespace awareness，军事用语。战场上，各级军事指挥官必须对各种信息有及时的掌握与深入的了解，从而做出正确的决策，因此绝对需访问各种分散的信息源并把这些信息综合到一起加以分析。于是 battlespace awareness 系统应运而生，它综合运用了各种高科技手段，如激光探测、化学和生物试剂检测、GIS、噪声和空气污染监控等。——译者注

系统)，但有些也比较复杂（如在地理上呈分布式的一套设备、系统、链接或节点）。比如，国防部管理着很多大型军事基地，包括海军的舰艇等，这些基地更像一座座小城镇，它们具有高压输电线、供热系统、空气过滤设施、自动化过闸设备、局域网、信息系统等，在轮船和飞机上还有精密计时仪器。

广义说来，DI 由下列事物和服务组成：信息与通信网、计算机、软件、数据库、应用程序、武器系统接口、数据、安全服务以及在军事范畴中能够满足国防部用户的信息处理和信息传输要求的其他服务。

DI 包括：各基地以及战略、国防等机构的信息系统，武器系统的指挥、控制、通信、计算机和情报接口，对声音、数据和图像进行收集、分布、存储、处理和显示的物理设施。

DI 还包括：各种应用程序和数据工程工具、方法和处理过程，用于对指挥和控制软件进行构建并维护；情报；监视和侦察；按需对信息进行访问和利用的任务支持人员。此外，DI 还涵盖了网络互联和互操作标准及协议，综合设计、管理和操作所涉及各类人员和资产。

DI 以有效的信息与通信为其依赖基础，它有着 NII（国家信息基础设施）所共有的很多脆弱性，但因其防御任务的特殊性，DI 还存在着一些其他方面的脆弱性需要处理。

打好基础，以实现（1）准备和防范；（2）检测和响应（内容 1~5）

为了评估并消除基础设施脆弱性以及关键系统、重要职能机构和装备遭到信息攻击的可能性，国防部已经制定了相应的行动计划，在联邦政府中，它是首批制定该类计划的实体之一。关键国防基础设施保护项目将通过关键基础设施保护参谋处来监督并平衡利用国防部现有的工作和职能，同时综合其他的相关项目（如 DIAP、关键资产保障项目、基础设施保障保护项目等），从而确保最终的成功。另外，国防部正率先就关键基础设施保护工作对其人员进行培训。

关键国防基础设施保护项目的各部分工作促进了国家计划中**准备和防范**以及**检测和响应**目标的实现。

#### 关键基础设施保护项目（CIPP）

国防部指挥、控制、通信和情报助理部长负责制定了国防部的 CIP 政策，他兼任很多职务：国防事务中 CIP 职能协调员、CICG（关键基础设施协调组）内的国防部代表以及国防部的 CIO（首席信息官）和 CIAO（首席基础设施保障官）。

国防部基础设施和信息保障主任负责领导 CICG 的国防协调子工作组。子工作组的成员包括国家和防御部门的各联络官以及特殊职能的办事处。它是 CICG 的一个固定子工作组，负责 CIGG 对国防事务的协调工作，其目的是针对各类环境包括危机、突发事件、被攻击、恢复和重建等的国防要求，协助国防事务中的职能协调员，提供基础设施服务并帮助制定基础设施服务相关计划。

国防部的关键基础设施保护计划是其达到 PDD63 要求、使关键基础设施保护制度化的工具和载体。国防部的期望是，关键基础设施保护中的所有方面均能实现制度化。

国防部副部长已经为部内每个领导单位都分配了各自的防御责任，各单位各司其职，责任明确，这是国防部在其职能运行的制度化、组织化过程中迈出的重要一步。通过这种组织结构的变革，国防部内的每领导单位都有责任用一种综合性、制度化的眼光来对待各自对应的国防基础设施。

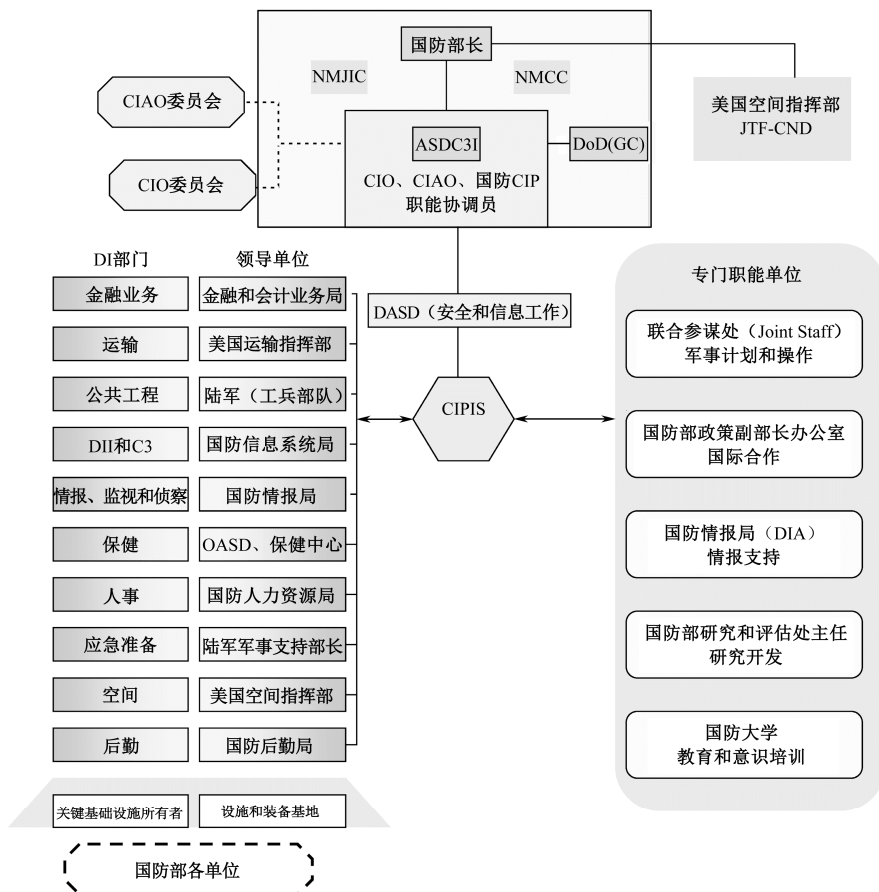
各类国防基础设施与国防部内领导单位的对应见下表：



国防基础设施（DI）部门	DoD 领导单位
金融业务	国防金融和会计业务局（DFAS）
运输	美国运输指挥部（USTRANSCOM）
公共工程	美国陆军（工兵部队）
国防信息基础设施（DII） 指挥、控制和通信	国防信息系统局（DISA）
情报、监视和侦察（ISR）	国防情报局（DIA）
保健	国防部助理部长办公室，保健中心
人事	国防人力资源局
应急战备	美国陆军（军事支持部长）
空间基础设施	美国空间指挥部（USSPACECOM）
后勤	国防后勤局

为了确保国防部各领导部门的计划制定和保障活动能够集成到一起，不至于各自为政，国防部副部长应 PDD63 和 CIPP 项目的指示建立了关键基础设施保护综合参谋处（CIPIS）。CIPIS 主要关注 DI 部门的整合、推进以及综合性的决策支持，在关键国防基础设施的保护中，综合性的决策支持扮演着积极而有效的角色，因为它使得在必要时间与地点的“集中保障”成为可能。

下图描述了国防部的 CIP 组织结构：



关键基础设施保护综合参谋处（CIPIS）

CIPIS 于 1999 年 7 月建成了其初步的运行能力。它负责监督并利用国防部现有的工作和功能，综合相关的 CIP 项目，并同私营部门建立合作关系。CIPIS 的成员有来自国防部各个 DI 部门的联络官以及联合参谋处、各军种和 JPO-STC（特别技术对策联合项目办公室）的代表。

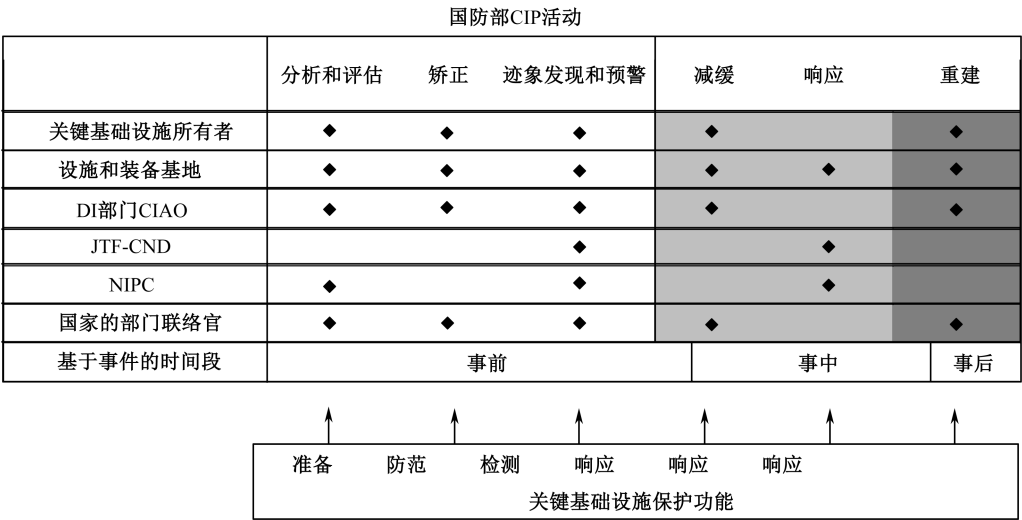
CIPIS 的职能有：确定现有军事计划中对国防部至关重要的基础设施资产；把国防基础设施区分为国家和国际防御基础设施；确保指定资产能够得到定性（qualitative）的脆弱性和互操作性分析；对指定的关键资产进行风险管理评估，向国防部的首席基础设施保障官（CIAO）和各单位推荐合理的安全措施；同 PDD63 中确定的国家各领导机构一起来协调 CIPIS 的结论和决策。

国防部内所有与矫正、迹象发现及预警、减缓、响应和重建工作相关的计划（如各国国防基础设施部门的计划、运营连续性计划等）、政策和步骤的形成也要通过 CIPIS 来协调。此外，CIPIS 还向 PDD63 所要求的那些涉及 CIP 的国防、国家安全和国际协调工作提供必要的专家和技术；此外，它还将寻求私营部门的支持，为各类国防基础设施提供专业技能、专家及意识培养活动。

方法

DoD 将通过 6 类保护活动来实现其 CIP 目标，这些活动可以划分为准备、防范、检测和响应功能。这些活动要得到有效的管理，从而确保它们可以在所有的实体间保持协调与和谐；各种操作建议能够得到交流；国防部关键资产所有者、设施和装备基地、各部门的首席基础设施保障官（CIAO）以及军事计划制定者和操作者均可以共享一个连贯的、信息丰富的、基于风险的决策框架。这些保护活动的目的是要保障国防部的正常运行以及任务职能，它们把物理保护和信息保障集成到了一个综合性的结构之中。

下图列出了上面提到的 6 类保护活动：



基础设施的分析和评估、矫正以及迹象发现和预警主要在事件发生前执行；减缓行为在事前和事中都要执行；响应行为在事中执行；而重建行为则始于事中，但一般来说主要集中在

于事后。每项活动均可以独立用于对物理和信息资产进行保护——物理资产是 DI 的依赖基础，而信息资产则构成了这些 DI 资产的“神经系统”。上图还显示了 DoD 和国家组织结构中各实体在不同阶段分别承担的主要保障或保护任务。国防基础设施部门的领导将为所有的关键资产建立每一保护活动阶段内以及在不同阶段过渡时的保护轮廓。

有几个实体的活动及职能横跨了所有的 6 类活动。国防部的 CIAO 委员会负责监督所有活动，并为它们提供资源和设定优先级。CIO 委员会将对 IT 矫正方案的开发以及它们在信息系统中的应用进行资助，并通过信息技术来促进减缓活动的开展。此外，它还将力图使 IT 的优势在重建活动中得到充分的体现和应用。

国防-CIP 职能协调员负责确定国家的基础设施部门中那些对国防至关重要的基础设施资产，并在国防部的整个活动周期内（指 6 类活动——译者注）为它们提出矫正、迹象发现、减缓及重建活动的倡议。此外，协调员还将监督各基础设施部门对这些资产的矫正活动，并在国家基础设施重建过程中表达和说明国防部的有关要求和权益。而且，协调员将在国家各基础设施部门内对减缓计划的制定做出倡议，并在所有级别上就国防部和国家活动之间的协调与交流发起联合的计划制定、培训和演习项目。

国家基础设施部门联络官的工作主要是协调国家基础设施部门的保障计划的制定和执行，并负责对基础设施特征化，他们还负责执行脆弱性评估并对相关活动进行监督和汇报。此外，他们将在每一基础设施部门内指挥减缓活动的计划制定、培训和演习，并监督各基础设施部门的重建活动。他们还将在必要的时候同 NIPC 一起进行信息共享。

### 分析和评估

分析和评估包括一系列连续性活动：关键资产确认、国防基础设施特征化、操作影响分析、脆弱性分析以及互依赖性分析。

国防部关键资产的定义是：对国防部在平时时期以及危机和战争时期的运行至关重要的任何设施、装备、服务或资源，国防部因而需要对它们采取各种措施和预防，以确保其职能能够连续、有效地履行并免于遭受各种不同程度的破坏，而且国防部还要对它们做到即时修复或重建（DoDD 5160.1，第 E2.1 段）。美国本土（CONUS）的资产将先于海外（OCONU）资产得到确定。在确定关键资产时，资产的所有权关系（公共部门、私营部门、美国政府、外资所有、多国所有）将不会作为制约因素。这种关键资产的确定是动态的，关键资产的名单将随着情况、时间和环境的变化而有所增删。

成就：DoD 已经开发了注册资产列表（RAL）——这是一个地理信息系统，包含了大部分重要物理地点和国防基础设施部门的资产。

请注意这里的活动只是对国防部所依赖的资产进行了确定，RAL 没有包括所有的国防及安全资产。

分析和评估时间表如下：

阶 段	活 动	目标日期
1.9	国防部关键资产拥有单位、国防基础设施部门的关键基础设施保障官以及设施和装备基地将确认其关键资产并执行初步的脆弱性评估。另外，DI 部门关键基础设施保障官将执行部门级的脆弱性评价，确认关键的部门资产	2000 年 8 月

续表

阶 段	活 动	目标日期
1.10	各国防基础设施部门和国防部关键资产所有单位将建立初步的方法和步骤，以用于物理安全脆弱性评估、技术援助、认证和认可、人事安全事件及计算机事件	2000 年 8 月

国防部关键资产所有单位有责任与 DI 部门的各个 CIAO 以及行动职能协调员和 CIPIS 保持协调，并在他们以及军事计划的协调下去完成资产级的脆弱性评估任务。国防部的行动职能协调员和行动单位将对行动的影响进行分析，确定军事行动涉及的关键资产。

CIPIS 将分析国防基础设施的互依赖性以及行动冲击，还将评估整个国防范围内基础设施的脆弱性。另外，CIPIS 还将确保国防基础设施特征化的通用性，对关键资产的确定工作进行协助，发起国防范围内的分析和评估，并为其他所有级别的活动提供技术和系统的支持与集成。

### 矫正

矫正是在意外事件之前采取的预防行动，能够改善已知的不足和弱点，从而确保国防基础设施部门或关键资产的运行或使其避免受到破坏。

比如，国防部的信息保障战略——纵深防御就是一例，它把国防任务进行了一系列分层，每层具有不同的强度和保障级别，并且每层都针对一个专门的目的。这些层中包括以下部分。

- 国防部广域网：加强对国防部广域网（WAN）的保护，防止计算机攻击，生产并配置一批稳健的加密产品；
- 国防部局域网：配置边界保护方案（如防火墙、护卫、病毒扫描器、入侵检测系统等）；
- 国防部主机、服务器、应用程序和操作系统：采用各种措施来阻止并检测非授权的行为，施行强访问控制方案；
- 重要管理业务；
- 强制性的雇员培训和认证；
- 标准化的 IT 和信息保障职位；
- 物理和计算机事件报表的综合与分析。

如上所示，该战略还考虑了重要管理业务的执行、雇员的培训和认证、IT 和信息保障职位的标准化以及物理和计算机事件报表的强化综合与分析。

矫正活动时间表如下：

阶 段	活 动	目标日期
1.18	国防部关键资产所有单位以及部门各关键基础设施保障官将提供矫正计划并为矫正计划提供资源。另外，国防部设施和装备基地将向部门关键基础设施保障官提供设施装备级的修复计划和资源	2000 年 11 月
1.20	DI 部门关键基础设施保障官将执行部门级的矫正措施，并整合和协调各部门内部资产级的矫正计划	2000 年 12 月
1.24	CIPIS 将整合并协调国防部门的矫正计划；评审国防部门的减缓计划和业务计划的制定；评审 DI 部门重建计划；起草综合的 DI 部门重建计划；起草各种有效性评测方案	2001 年 3 月

续表

阶 段	活 动	目标日期
1.28	各国防部门将完成与基础设施依赖性和国家国防基础设施关键性评估有关的风险管理原则的制定和应用。完成这一任务将依靠：制定并实施一致的风险管理框架；确定风险和不确定性来源；确定因果关系；认识可能性和结果的影响范围；评估极端事件；考虑极端事件带来的风险；确定和分析各个可能的选项	2002 年 12 月

### 迹象发现和预警

迹象发现和预警包括了各种准备活动或对基础设施状态的分析，这些状态往往能显示出是否存在可能的计算机事件以及事件目前的状态（是处在计划阶段还是已经开始）。

DI 部门 CIAO 将负责制定并执行 DI 部门的事件监控和报告的过程及步骤，国防部关键资产所有单位和国防部设施和装备基地则将参与到基础设施事件的判断、监控和报告行动中。国家军事指挥中心（NMCC）和计算机网络防护联合特别任务中心（JTF-CND）将负责接收、联合并评估部门报告；通过把部门报告与传统的情报信息相融合，制定出国防部的事件迹象报告；把这些迹象报告汇报给 NIPC；发布警报；对国家预警进行接收、评估和传播。

CIPIS 负责提供技术集成和支持。国防部研发职能协调员将为检测工作提供改良的材料、工具、方法和模型。DoD 情报支持协调员将为部门 CIAO 提供专业的建议、帮助和支持，使他们能够制定并执行监控和报告活动。

NIPC 在此处的角色包括：指导国家对迹象发现提出要求；参与设计与发展国家各基础设施部门的监控和报告能力；接收、联合并评估各基础设施部门的报告；通过融合各基础设施部门的报告与传统情报，制定事件迹象报告；发布国家预警。

成就：通过在关键系统节点安装入侵检测系统并建立 24 小时的监视，国防部已经大大提高了其对系统状态的判断和标识能力，并且能够把情报信息与通过监控得到的信息融合到一起。

### 减缓

减缓是由国防部关键资产所有单位、国防部设施和装备基地、DI 部门以及军事指挥部门所采取的行动，是对基础设施事件预警的响应。

国防部关键资产所有单位以及设施和装备基地将制定资产级以及设施装备级的减缓活动，并为这些活动提供培训和演习，所有这些活动都是对警报、紧急事态和基础设施事件的响应。而且，关键资产所有单位和设施装备基地还将负责把减缓状态向 NMCC、JTF-CND 和有关的部门 CIAO 汇报。部门 CIAO 将整合并协调部门内的资产级减缓计划和活动，并把减缓状态向 NMCC 和 JTF-CND 汇报。NMCC 和 JTF-CND 将监控紧急事态和事件，向受到影响的有关国防部实体和单位提供减缓状态，并建议或指导减缓行动。CIPIS 将为 NMCC、JTF-CND 和部门 CIAO 提供技术集成支持。

NIPC 将监控国家级别的紧急事态和事件，向受影响的国家实体提供减缓状态，并对减缓行动做出建议。

成就：通过信息保障脆弱性报警（IAVA）项目，已经针对信息系统的风险确认和修复而建立了积极的控制手段。

## 事件响应

事件响应指那些消除事件起因或事件源的活动，包括由第三方（即非资产所有者和操作者）采取的应急措施，如执法、调查、医疗、消防和营救等。

事件响应时间表如下：

阶 段	活 动	目标日期
1.19	国防部关键基础设施部门 CIAO 将监控响应活动，协调相关部门的减缓及重建活动，并为国家军事指挥中心(NMCC)提供支持	2000 年 11 月

国防部关键资产拥有单位和设施装备基地将与适当的响应实体进行协调，并为局部响应制定计划，同时负责局部响应的培训和演习。计算机网络防护联合特别任务中心（JTF-CND）将针对那些影响到其国防范畴内的资产的事件进行响应。CIPIS 将为 NMCC、JTF-CND 和部门 CIAO 提供技术支持，并监控响应活动的状态。NMCC 也将负责对响应活动的状态进行监控。

成就：对计算机应急响应组进行了扩展，使其能执行报警、受害系统甄别分类以及修复任务；制定了应急计划来缓解网络遭到的破坏或损失。

## 重建

重建指在基础设施遭到破坏之后对其进行的重新组建或恢复工作。

在国防部设施和装备基地的支持下，国防部关键资产所有单位将负责对资产进行重建并向部门 CIAO 报告重建状态。部门 CIAO 将监督重建活动，同 NMCC、JTF-CND、NIPC 和 CIPIS 共享信息。另外，部门 CIAO 还将执行部门级评审，资助或发起 CIP 步骤的改良活动，以及更新 DI 部门的特征化结果。

JTF-CND 将监督其国防范围内的资产重建工作并对这些工作提出建议。另外，它还将在完成行为分析后向部门 CIAO 和受害单位提供响应信息，供重建时考虑。CIPIS 在其同私营部门的合作关系和工业界专家的支持下，将可以向 NMCC、JTF-CND 以及受害单位和部门 CIAO 提供技术支持。NIPC 将提供事件响应评审结果，供制定重建计划时采用。此外，它也将监督重大的国家基础设施重建工作。

FEMA（联邦应急管理局）将作为应急服务的领导机构，根据联邦响应计划，负责国家应急响应的后果管理。

## 关键国防基础设施和信息保障系列项目

在基础设施和信息保障主任的指导和监督下，CIPIS 将对如下一系列项目进行整合并提供监督。

### （1）国防信息保障项目（DIAP）<sup>①</sup>

DII（国防信息基础设施）的任何一部分都面临着风险和脆弱性，这已经威胁到了所有单位的运行和行动，为此，国防部审时度势，迅速采取了针对行动，以确保其信息的可用性、完整性、真实性、保密性和不可否认性，并努力对其信息基础设施提供保护。最近的很多评

① 关于 DIAP 和 IAP 的详细说明可参见 <http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm> 的附录 F 及附录 E。——译者注

估、演习（即“合法接受者 97”<sup>①</sup>）和真实事件清楚地表明国防范畴内的信息保障（IA）工作是绝对不可少的，而且，这项工作要不断地开展和提高。我们再也不能靠事后解决方案而沾沾自喜了。国防部已经对其信息基础设施施行了现代化，但它仍需再接再厉，继续在研发、产品的实时集成、行动步骤以及培训等方面进行投资，确保国防部有能力保护其自身。在国防部所有需要优先考虑的活动中，DII 保护是其中之一，同时也是一项最为艰难的挑战。

我们要有一个全国防部范围的计划及综合框架，它的执行对于国防部的 IA 目标——持续地提供可用性、完整性、真实性、保密性、不可否认性，并能够使 DII 的重要部分在破坏后能够迅速恢复来说至关重要。为此，国防部副部长在 1998 年 1 月批准成了 DIAP，从而得以作为 DoD 的信息保障活动和资源利用制定计划并进行协调、整合和监督。

DIAP 形成了国防部 IA 项目的核心部分。它提供了集中式的监督，但同时又保持了分散式的执行，从而使我们的 IA 工作不断发展和进步。DIAP 的集中式协调与监督有如下好处：使国防部得以准确地开发、确认、整合及优化 DoD 范围内的 IA 要求；可以观察到 IA 投资的结果并对其进行判断；能够客观地评价我们整个的国防体系为保护 DII 和 NII（国家信息基础设施）及 GII（全球信息基础设施）的关键组件所作的努力。而合适的构建与执行方式（指分散式——译者注）则使得 DIAP 既能够实现其必要功能，又对当前和未来的各类 IA 事项、威胁和脆弱性保持足够的响应能力。虽然 DIAP 提供了通用的管理框架与集中式的监督，但这一大项目中每一子项的执行仍是各个战区司令官（CINC）<sup>②</sup>、各军种和国防部各机构的责任。

信息保障要求的方法和途径超越了传统的国防部信息保护方式。传统的方式主要基于国家安全方面的考虑，而现在的这种信息保障途径必须研究各种信息对机构职能任务运行的关键性是何种级别，并提供与这种关键性相称的保护措施，从而确保这些信息在传输过程中不会被破坏，还要确保它们的可用性，以在需要时对关键基础设施提供支持。IA 是一门不断发展的、动态的学问，因此它要求对新出现的技术以及变化中的脆弱性和威胁具有灵活性、可适应性和响应能力。DIAP 的建立说明了整个国防部已经逐步懂得了 IA 的动态特点，并认识到了正是人们对互联、互依赖系统和服务的日益依赖才造成了现在这样一个所有人都面对的风险环境，这种风险环境迫使我们必须在国防部内开展前所未有的协调和统一工作。

DIAP 由国防部指挥、控制、通信和情报助理部长办公室信息保障委员会负责，其工作人员来自于国防部各机构、现役军和后备军、情报共同体。DIAP 的工作班子得到了以下几个 DIAP 联络中心的支持：情报共同体（IC）协调中心、关键基础设施保护（CIP）综合联络处、联合参谋处联络中心。DIAP 的初等运行能力（IOC）是于 1998 年 6 月建成的。

DIAP 由两个小组构成：职能评估和整合小组（FEIT）以及项目发展和整合小组（PDIT）。FEIT 包含 8 个职能领域，涉及项目活动的发起、协调及监督。每个职能领域中都有一个小组长（team leader），负责发起、协调、评估职能领域内部以及职能领域间的组织活动。FEIT 的 8 个职能领域分别是：预备工作评估、政策监督和执行、人力资源开发、体系结构标准和

① 这是发生于 1997 年的一次演习活动，展示了黑客如何通过渗透进国家安全局来破坏城市的“9·11”服务和电话网。这次演习暴露了大量的安全弱点和脆弱性，引起了政府和国会和信息战的关注。有关资料可见 [http://www.infowar.com/civil\\_de/civil\\_022698b.html-ssi](http://www.infowar.com/civil_de/civil_022698b.html-ssi)。——译者注

② 美国军事力量划分为 10 个主要司令部，各由其战区总司令（人们称之为“辛克”，即英文“总司令”的几个单词的首字母缩写“CINC”的发音）指挥，且至少是四星将军。——译者注

系统变换、采购支持和产品开发、安全管理、行动监控和事件响应以及技术和研究。每个职能领域均受到其小组的支持，小组将把其活动结果同 DIAP 的 PDIT（项目发展和整合小组）联系起来，供国防部的计划、规划和预算系统（PPBS）<sup>①</sup>使用。

PDIT 为国防部的 IA 资源提供监督、协调和整合服务。通过使用由 FEIT 提供的项目方针以及其他信息，PDIT 确保这些信息能够在各单位间发布和传达。PDIT 将对各单位的 IA 计划、活动和资源投资进行监控，并评估资源的有效性，从而确保 DII 的运行以及 NII（国家信息基础设施）和 GII（全球信息基础设施）对其提供的支持。PDIT 还负责为国防部 IA 的花销基准做出记录，这些花销包括那些用于信息系统安全策略（ISSS）的资金以及国防部其他 IA 项目所花费的资金。

### （2）IAP（基础设施保障项目）

关键基础设施保障项目（IAP）是一项研究和工程学项目，它由国防部长办公室（OSD）和联合参谋处发起，始建于 1995 年。美国海军是其执行服务军种，特别技术对策联合项目办公室（JTO-STC）负责对其管理。IAP 花费了 DoD 迄今为止的大部分相关投资，不论时间还是资源，来研究解决国防部对商用关键基础设施的依赖性问题。作为这项工作的成果，我们深入研究了其他方式方法，建立并验证通过了专门适合于国防部任务需求的处理过程和操作步骤。这套为国防部的关键基础设施保护而设计的过程和步骤将依靠 JPO-STC 的关键基础设施保障项目（IAP）的支持系统，并且还要将 JPO-STC 的 IAP 支持系统进行扩展，使之能够解决国防部所有基础设施的需求。

IAP 可以为国防部的基础设施保护工作做出如下贡献：

- 研究 CIP 分析和保障周期（关键资产确定、国防基础设施特征化、行动冲击分析、脆弱性评估和互依赖性分析）内所有活动所使用的工程方法、工程基准和工程工具，这些方法、基准及工具要能够适用于所有的级别（资产级、设施装备级、国防基础设施级、军事行动级以及整个国防范围级）。
- 为基础设施独立性分析提供集中化的国防部专家和技术；为把国防部关键资产和国防基础设施映射为国家和国际防御基础设施而提供集中化的专家和技术。
- 开展基础设施信息安全研究，制定标准；向军事计划、操作和情报提供分析和集成支持；信息工程学研究。

### （3）公钥基础设施

公钥基础设施（PKI）由各种可以对公钥证书进行产生、制造、发布、控制和账户处理等操作的框架和服务构成。对于公钥技术的大规模、可互操作性用法来说，PKI 显得尤为必要，它可以支持数字签名、保密性以及其它安全服务，从而促进信息的可信电子化交换。因为 PKI 产品和服务已经在商业市场上得到了开发，像其他联邦机构一样，国防部也对这些产品和服务进行了采纳并经过了必要的改动，以图最大程度地利用这些商业产品和服务，尽可能地减小政府在这方面的昂贵投资。国防部已经建立了很多 PKI 试验项目，希望这些试验活动能够推动对大规模的 PKI 上马时将出现的诸类问题和挑战的理解和认识。

① PPBS 是在国防建设中为了达到合理地分配和使用资源，对规划、计划和预算进行系统管理的一种方法，又称规划计划预算综合编制法。它把规划、计划和预算视为一个整体系统，致力于整体最优而非局部最优，是系统工程方法实际应用的范例。美国国防部在 20 世纪 60 年代初率先采用，60 年代中期逐步推广到政府其他部门和企业界，如今也是哈佛大学的教育课程之一。——译者注



为了确保国防部用户之间的互操作性，使操作损耗减至最小，国防部将采用一套具有集中式管理结构的 PKI 系统，同时这套系统还要支持外部资源利用（outsourcing）和某些 PKI 组件的分布式操作。企业级的 PKI 系统将涉及众多的安全令牌技术，它同时支持商业和联邦标准，能够满足国防部内部以及国防部与私营部门单位之间的安全电子交易的全面目标。

为了使国防部的 PKI 工作得到更多关注，PKI 发展路线图和 X.509 证书政策均已问世。这些文档的制定有助于用户和提供商更好地认识国防部的 PKI 目标与宗旨，同时他们也是 PKI 的执行战略和关键技术及过程的发展时间表。在 1999 年 4 月，为了加强管理和监督，国防部助理部长（负责指挥、控制、通信和情报）将国防部的 PKI 管理任务交付给了国家安全局（NSA）和国防信息系统局（DISA）来承担，项目总管来自 NSA，副总管来自 DISA，项目管理办公室则位于 NSA。

此外，国防部副部长还在 1999 年 5 月 6 日制定了部级的 PKI 政策，以为之提供服务基础和机构战略，从而对国防部的 PKI 目标的最终实现起到支持作用。国防部的 PKI 政策如下所列：

- 强调信息优势的重要性，要求国防部的 IA 功能要能够处理信息、信息系统及基础设施的多样性与遍布性问题，支持战时和日常业务的运行。
- 尽可能多地在适当的地方采用 COTS（商业现货）技术，以紧跟技术的发展，只在必要的时候才开发 GOTS（政府现货）解决方案。
- 建立国防部 PKI 的实施时间表，满足所有 IA 服务的要求，鼓励对可支持 PKI 的应用程序进行广泛支持，为在整个国防部范围内采用 PKI 服务提供专业的指导方针。

国防部 PKI 实施计划时间表如下：

阶 段	活 动	目标日期
1.25	使用经签名的电子邮件。所有电子邮件都将被签名，在整个国防部内鼓励对邮件进行加密	2001 年 10 月
1.27	国防部将向其所有 PKI 用户发行最安全的证书/令牌	2002 年 1 月

检测和响应（CIP 工作中很重要的部分）（内容 2~5）

迄今为止，国防部与其他联邦机构和私营部门的 CIP 工作之间最显著的不同是，国防部在其所有的关键节点中配置了入侵检测系统（IDS），并且对高级 IDS 做了不断的开发，并建立了 JTF-CND 组织来管理这项工作。

入侵监控系统（增强性功能）

有几类入侵检测系统正在整个国防部内使用，其中有些是 GOTS 产品，也有些是 COTS 产品。前者主要分为以下几类：网络安全监控器、网络入侵检测系统、联合入侵检测系统。

- 网络安全监控器产品用来观察网络流量，检测非授权的网络活动，并提供实时报警。
- 网络入侵检测监控产品是一套可以用来检测、分析和确认网络入侵行为的软件工具。
- 联合入侵检测系统结合了网络安全监控器产品和网络入侵检测产品的最优特性。

入侵检测研究领域目前正在开展的另一项工作称为先期概念技术演示<sup>①</sup>自动化入侵检测环境（AIDE-ACTD）工程。该工程旨在演示各类设备对入侵活动进行检测、显形和报告的能

① 先期概念技术演示（ACTD）项目是在先期技术演示（ATD）的基础上发展而来的，目的是为加速将实验室中的新技术转化为战场上实用的武器装备。——译者注

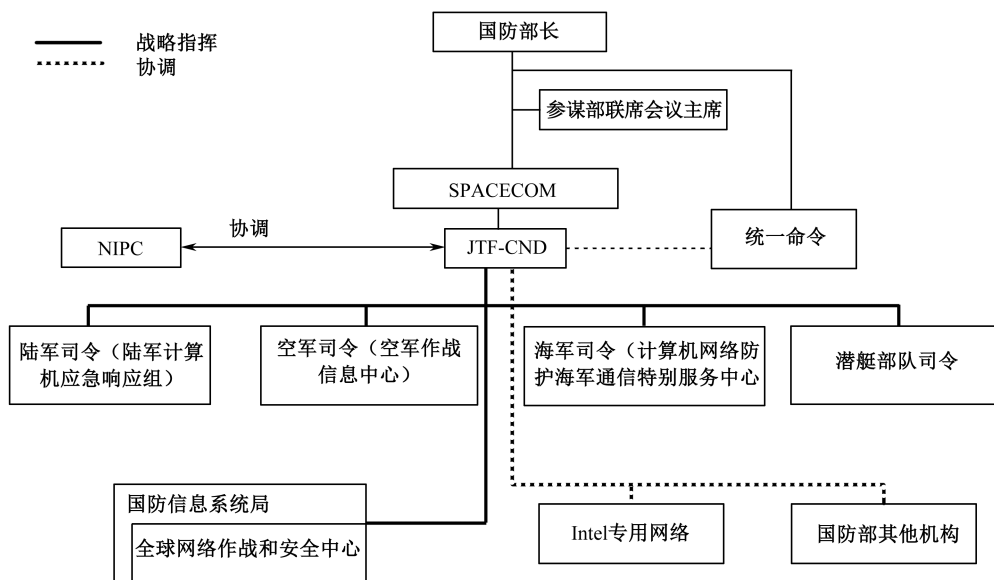
力，目标是发展一种能够对系统是否正在遭受入侵进行判断的功能。这一项目将为我们提供自动化的检测、关联、警报和报告手段，以用于综合的威胁报警和攻击评估。分散于各处的信息系统感应器设备将充分利用从各军种和国防部机构处收集的攻击事态汇报及攻击模式，这项技术可以使我们能够辨别出群攻击，并把那些看似正常的黑客攻击行为过滤掉。我们的下一步目标是把各类相异的感应器的服务功能集成到一起。

### 计算机网络防护联合特别任务中心（JTF-CND）

JTF-CND 负责监控计算机事件和潜在的威胁，协调国防部的工作，为阻止攻击或控制破坏并恢复网络功能而制定相关的活动计划并对其做出指导。

JTF-CND 的主要功能是：使针对计算机网络攻击的技术、操作和情报评估工作相同步；评估计算机网络攻击对军事操作和功能带来的冲击，并向国家指挥中心（NCA）和用户团体通报；协调并指导相关的国防部活动，以阻止攻击、控制破坏程度、恢复系统功能并向用户团体提供反馈；评估防御行动的有效性；在需要时与国家通信系统中心（NCS）、位于 FBI 的 NIPC、DoD 的执法局（LEA）、DoD 反情报组织、民事执法机构、其他跨机构合作系统、私营部门以及各同盟保持协调。

在 1999 年 10 月 1 日，美国空间指挥部（SPACECOM）成为了 JTF-CND 的指挥机构。下图描述了 JTF-CND 的指挥关系：



JTF-CND 并不是一个决策机构，但是在必要的时候它也将参与政策的制定。JTF-CND 不负责处理计算机网络攻击事件，它的工作人员只是监控每日的网络运行情况，为后面的危机处理站好第一班岗位。

成就：1998 年 12 月 30 日人们建成了 JTF-CND 的初步运行功能。

## 国防部在国家事务中的角色

应行政令 12333 (EO12333) 的指示, 国家安全局 (NSA) 局长将为美国政府的通信安全负责。在 42 号国家安全令 (NSD-42) 中, NSA 局长还要履行国防部作为政府的行政机构所担当的国家安全电信和信息系统安全职责, 且 NSA 局长还要负责 NSA 对国家安全电信和信息系统安全的管理工作。国防信息系统局 (DISA) 局长则负责国家通信系统中心 (NCS) 的管理。NCS 是应肯尼迪总统于 1963 年 8 月 21 日签署的总统备忘录而开始筹建并运行的。1984 年, 第 12472 号行政令《国家安全和应急战中电信职能的分配》的发布改变了 NCS 的任务重心, 使其从制定计划和协调政府单个通信系统的职能转移到了其现在的任务职能, 即: 协助总统和总统行政办公室 (EOP) 的战时及非战时电信应急响应, 协调各种环境下联邦政府的 NS/EP (国家安全/应急战备) 通信计划和条例的制定。

### 计算机应急/计算机事件响应功能中心

很多年以前, 国防网络就开始经历越来越多的威胁国防部信息系统网络的计算机安全事件。为此, 国防部发起了很多相关的行动来对这些事件进行报告和监督。另外, 为了保持其机构运行的有效性, 国防部还组织了专家组以响应计算机事件并对这些事件造成的破坏进行弥补。自此以后, 很多计算机应急响应小组 (CERT) 和计算机事件响应小组 (CIRT) 在整个国防环境内成长起来。

国防领域的各个军种和机构的 CERT/CIRT 同全球网络运行安全中心 (GNOSC) 之间均存在着相互联系。后者是国防部的企业级 CERT, 也是国防部同其他政府机构和私营部门的 CERT 相互交流的窗口。国防领域的各 CERT 均有一套明确的步骤和过程来定义和报告事件数据并实现信息共享和与响应职能的互为补充。在 JTF-CND 结构内, GNOSC 负责提供 CERT/CC (计算机应急响应组/协调中心) 服务, 保持 DII 及 NII 的互联系统及 Internet 的安全性和稳健性。

国防领域内的大多数 CERT 是事件响应和安全小组论坛 (FIRST) 的成员——FIRST 是一个国际联盟, 由全球各地的很多政府和私营部门组织构成。

成就: 国防部和各军种之中已经建立了多个 CERT。

### 对国家基础设施保护中心 (NIPC) 的支持

国防部在 NIPC 内有一个分遣队, 负责确保国防部关键基础设施保护中的情报、反情报和执法职能的顺利开展。作为 NIPC 的一部分, 国防部分遣队也将执行国家范围内的互依赖性和脆弱性分析, 定义国家的迹象发现需求, 负责接收、联合和评估各基础设施部门的报告, 监督国家的应急和事件响应, 另外还要监督重要的国家基础设施重建工作并在必要时协调国防领域内的其他相关活动。

成就: 经过国防部与 NIPC 和执法机关之间的工作努力, 人们已经建立了用于同私营部门共享关键基础设施保护信息的步骤和过程。

### 建立坚实的基础

新技术的发展同时也带来了新的危险, 没有人怀疑我们的信息基础设施正处在很多危机之中。在一系列的演习以及实际攻击事件中, 国防部已经看到了第一波计算机攻击浪潮的涌

起。长久以来，国防部就一直注意在这一领域开展不懈的研发，最近发生的一些事件更促使它加强了对计算机威胁响应的研究工作。

### 信息系统安全战略（ISSS）

信息系统安全战略（ISSS）是 DIAP（国防信息保障项目）的核心部分。该战略具有多角度、多层次的特点，直接针对的是新型或增强性的 IA 操作功能的运行以及高级 IA 技术和系统解决方案的配置，该战略还将强化国防部各类人员的 IA 技术和能力。

在信息系统安全和信息保障政策、标准及体系结构的框架内，DoD ISSS 为 DII（国防信息基础设施）的纵深防御考虑了集成式的保护层次。它们包括确保应用程序的安全、保护主机和主机附属系统的安全以及保护网络的安全。此外，要坚持执行《安全技术执行指南》和《安全手册》并做到时常更新，还应落实并配置网络入侵检测系统。

NSA、DISA 和各军种在该领域内还开展了很多其他的项目。而且，因为信息保障解决方案的正确配置、使用和维护对我们的网络和系统的安全来说至关重要，这些方面也正受到越来越多的关注。

### 同国防相关的研发活动（内容 6）

国防部的关键基础设施保护研发（CIP R&D）计划将充分利用国防部和联邦政府现行的研发项目，制定出一个基础设施及信息保障保护研发活动框架，为国家的其他研发活动提供相互间的补充和利用。

国防研究和工程局局长办公室（ODDER&E）将同国防部的 CIAO 以及 CIP 联合参谋处、部门 CIAO 和各军种/国防部各局的研发活动相协调，以制定国防部的 CIP 研发计划，满足国防基础设施部门和关键互依赖性研发的需求。此外，它还将同 DIAP、CAAP、IAP 和其他的 CIP 相关项目中的现行研发活动保持协调和磋商。

作为国防部的代表和国家 CIP 研发跨机构工作组联合主席团副主席，国防研究和工程局局长将向国防部的 CIAO 和 CIAO 委员会提供反馈和建议，协调国防部和国家之间的研发日程，并代表国防部参与国家研发日程的制定和执行。

#### （1）DARPA（国防高级研究计划局）的研究活动

从 1995 年开始，国防高级研究计划局/信息技术办公室（DARPA/ITO）就开始了对于长期研发投资战略的探索，以开展信息系统生存力技术的研究。该战略的第一阶段是信息生存力项目（1995—1999 年），这一项目弥补了 4 个领域内的空白：迹象发现和警报（I&预警）、保障和集成（A&I）、高度可靠性网络、计算科学。

ITO 的第二阶段投资称为内在生存力项目。该项目将建立在前面的信息生存力项目之上，其重心从上述的 4 项技术主题转移到对后续挑战层的关注，从局部入侵检测转移到全局入侵评估，从加强对渗透的阻拦转移到对试图击破这些阻拦的攻击行为的抗衡与承受。

#### （2）信息保障项目

国防部高级研究计划局的信息保障项目主要考虑对信息系统的日益依赖问题，并确保“正确的人在正确的时间获取正确的信息”。我们所处的环境对信息的传递和保护以及相关服务可用性有着强烈的需求，因此上述考虑是非常必要的。信息保障技术将集成到 DII LES（国防信息基础设施前沿业务）的未来版本中，为整个国防部信息系统提供稳健的体系结构。这

一项目希望能够开发出藉以减少信息脆弱性的安全框架，同时该框架还要能够提供强化的互操作性和相关功能，使行动指挥官可以及时得到所需信息。

新出现的战略性计算机防御<sup>①</sup>概念就是建立在如上基础之上的，它主要探索了信息保障中的6个关键领域：信息保障科学和工程原理、计算机感应器和入侵检测系统的开发、计算机和网络状态的跟踪和分析、计算机系统指挥和控制工具、防护机制、计算机防护战略。

### （3）解决方案的产生和发展

为了迎接网络环境和 COTS 产品带来的挑战，国防部已经在其很多研究活动中同工业界结合在一起，把工业界看成了其全面的合作伙伴。这些合作活动包括：开发网络安全框架；发展和制造网络安全产品；继续维护和强化传统的安全产品套件，在商业界的解决方案匮乏或不奏效的时候使用。

### （4）NSA（国家安全局）研究活动

国防部的系统和网络的安全性依赖于我们对系统及网络的脆弱性了解和掌握的能力。NSA 拥有大量脆弱性检测方面的专家，可以提供脆弱性分析支持，它还可以判断安全措施充分性、评估安全弱点、为预知特定安全措施的有效性而提供必要数据并在这些措施执行后对其安全性能做出全面结论，而且，NSA 还可以发现、调查和记录现有及发展中的网络技术中存在的安全脆弱性。

NSA 诸研究项目的目标是确保 IA 解决方案始终紧跟领先的信息技术，并向客户提供重要的安全服务。它研究的技术领域包括主动式网络防御、安全网络管理以及网络安全工程学，所有这些技术均要得到密码和安全通信方面的研究支持。

主动式网络防护为国防信息作战（DIO）提供了研究及高级技术开发资源。这些现行的和未来的研究工作将开发出新型的工具和技术，用来分析各类攻击，指出它们的来源和意图，还要研究相关技术以支持人工和自动化的响应。在未来的网络攻击可视化研究工作中，我们将开发出可以显示多变量数据的原型来，以应付与超大规模系统相关的数据集。在目前已启动的一项新工作中，我们的研究希望能够实现针对各种不同的入侵模式来自动采取合适的网络响应的系统。流动智能体的研究中将调查这项技术在网络攻击检测和响应中的可用性。

安全网络管理将为信息共享、网络控制和信息系统事件监控而开发安全协议，从而对安全管理基础设施（SMI）的操作提供支持。未来的研究工作将制定出安全性得到必要强化的 Internet 协议规范以及执行参考，并支持国际范围内的标准化团体。其他一些在研项目将分别关注下列课题的研发：多播的安全但非密码类技术、多点传送路由的安全机制、群密钥管理服务。

网络安全工程学要解决的很多问题对于安全软硬件和网络系统的开发来说是非常重要的。其中，系统边界研究领域内的工作将主要关注网络边界的确定和保护，从而为对付计算机攻击而建立起一系列的监督、控制和防御点。当前，边界保护的主要手段是防火墙，它基于地址数据对通信流进行过滤。而新的研究期望能开发出高性能的边界保护设备，就数据本身或专门协议来过滤数据流。我们的宗旨是高效和高能，尽可能提高数据过滤速率。其他的研发活动中还包括了对高级 ATM 网络交换技术，如 IP 交换的安全性能的评估。另外，网络

<sup>①</sup> 战略性计算机防御对我们一般所说的“响应”进行了概念上的发展，它强调反击，更加着重于定位攻击源及提供攻击证据。此外，它比“defensive”概念更具攻击性（offensive）色彩，属于新出现的“cyber forensics”（计算机法学）学科的研究范围。如需细节知识请参阅《战略计算机防御概念白皮书》，<http://www.isi.edu/gost/cctws/tiren.html>。——译者注

安全工程学也将研究同对象技术的使用相关的诸类安全事项，且这项研究工作将会通过对象管理组（OMG）来完成。

所有的军种及国防机构均同 DARPA 和 NSA 有着密切的合作，以便于使其研究结果能够在实际的操作环境中得到运用。这些实际操作环境包括：指挥、控制、通信和计算机环境；情报、监视和侦察系统；武器系统；战区级网络管理；战术作战能力；网络和基础设施生存力等。另外，各军种、NSA 以及 DISA 均还有其他的对应项目，用来支持研究以及技术、基础设施和人力资源的发展。

#### **教育、培训、意识培养和职业化（内容 7）**

在国防部的信息和基础设施保障活动中，受过培训与激励的人力资源对活动的成功起着决定性作用。国防部系统的高度互联和互依赖性造成了现在的这种公共风险，因此，国防部系统的所有使用、管理、维护人员必须理解国防部系统所面临的威胁，并明确为了减弱这种威胁而设计的有关政策、步骤和设备。

国防部的很多法规和条例中都要求对使用国防部计算机系统的雇员进行培训。培训及职业要求在 IA（信息保障）和 IT 技术的基准评估说明中阐述。当前，一系列连贯的正式 IA 培训和认证计划正在实施之中。各军种、NSA、DISA 都设立了培训中心，这些中心将会紧密合作，提供广泛的培训，使雇员达到规定的要求。

成就：加密系统的用户、系统管理员以及系统维护人员必须在 1999 年 1 月前通过认证，非加密系统则要在 2000 年 12 月前完成这项工作。

国防部的 Infosec（信息安全）项目开发了一系列（到目前为止是 17 套）光盘和录影带，供整个联邦政府使用。这些材料的内容包括国防部信息战基础、国防部和联邦政府的 INFOSEC 意识培养、信息时代的技术（IT 基础设施概览）、审计和评估人员的信息保障教育、风险中的网络认识以及黑客入侵描述等。

#### **演习和红队的模拟进攻**

如同本计划的其他部分所提到的，千年虫危机促使我们迅速制定了演习行动计划。在国防部和联邦应急管理局（FEMA）的联合领导下，人们针对千年虫危机进行了大量的演习。

这些演习测试了千年虫事件可能对国家安全带来的危机，使我们知道了如何分配稀有资源，并考验了联邦各机构所制定的针对性计划的效果。

本篇国家计划对演习工作完全支持和赞同。另外，联邦政府的所有机构都同私营工业的部门协调员合作参与了定期的演习活动，这些演习活动主要关心系统安全、入侵响应、重建方法以及计算机危机中的全面管理。

国防部的红队将继续对安全措施进行测试。通过红队的模拟攻击试验，国防部可以确定一致的目标和通用结构，并将得到很多有意义的可比性结果。此外，红队项目还将对 IA 过程、系统和组织进行周期性的独立评估，从而对脆弱性提出公正的评价。

对很多重要的国家安全系统或网络来说，不能要求外部力量对其进行脆弱性评估。出于安全的考虑，这些测试要依靠内部小组来完成。

#### **培育公共-私营合作关系（内容 8）**

为了保护我们国家的关键基础设施，培育政府-工业合作联盟以及同私营部门进行信息共享是必不可少的。关键基础设施保护综合参谋处（CIPIS）在国防部的 CIP 组织结构中占中据中

心位置。同时，国防部的设施和装备基地担当了“国防部同设施所在国、联邦、州及地方执法机关、应急服务人员和商业基础设施提供商之间相互交流的窗口”。

CIPIS 将与 ISAC（信息共享和分析中心）合作，建立起国防部同这些支持部门的合作关系。在国防基础设施（DI）内，CIPIS 将在与私营部门代表的合作下定义国防部和私营部门之间的信息（包括加密信息以及商业秘密等）交换步骤。这种级别上的信息共享可以通过双方的协定、开放式论坛或其他交流方式来完成。

在国防部的设施装备级上，政府以及私营部门的 DI 代表将在一起合作，共同实现国防部内领导单位/CIPIS 在其评估计划中确定的需求。政府/工业界的代表将在各级地方政府和相应的私营部门参与的基础上针对设施和装备基地的职能运行需要而提出他们的建议。这些代表还将为当前的某些政府/工业界合作关系典范，如国家安全电信顾问委员会制定信息交换的执行步骤。

### 推动国际合作

为了追求 CIP 事务和信息交换中的国际合作并与其他国家、国际组织、多国联盟的 CIP 项目相协调，有很多事情还有待我们去完成，包括：改进美国本土之外的军事及支持基地的基础设施保障和应急计划的制定；支持情报活动；促进事件相应的协调；理解全球化对美国基础设施带来的冲击；确保当前及未来的 CIP 和（或）IA 国际协定中以适当的方式包含了国防安全服务局（DSS）的执行机制。

CIPIS 将在国防部的 CIP 过程中把国际协定考虑进去，并协调新出现的有关需求。DSS 将参与 CIPIS 的工作，为国际上工业界的安全协定的执行提供建议和支持。

## 5. 私营部门以及州和地方政府的关键基础设施保障框架

### 公共-私营合作联盟的需求

只靠联邦政府自己是无法保护国家的关键基础设施的。私营工业和州及地方政府直接拥有并有效控制着对国家安全和经济利益极为重要的大量基础设施，它们可以对基础设施产生巨大的影响。因此，只有同工业界和州及地方政府之间实现有效的合作，联邦政府才可以保护好这些关键基础设施；相反，如果单枪匹马，则必然失败。

这并不是说，在保护私营部门的基础设施中，联邦政府没有或只有有限的角色。我们这样说的意义在于，联邦政府必须通过合作的手段来采取行动。它应该力促私营部门投入到保护行动中，共享威胁信息和矫正手段；还应支持私营部门去设计并执行自己的防护项目，为它们减少行动的障碍，激励它们从事重要的研发；另外，在必要的时候，为它们提供综合性领导。联邦政府同私营部门基础设施提供者应当是一种全面的合作关系。

### 合作的原则

- 自愿。
- 基于共同的着眼点，合作是为了取得清晰、集中而明确的目标。
- 合作关系应能弥补彼此的弱点，强化彼此的功能和角色。
- 对于彼此的价值观、期望、要求、关注事项和目标的理解。
- 持续不断地相互交流。
- 共同的信任。

➤ 要有经过充分计划的出发点。

这种合作关系应当是积极而自愿的，并且要由各参与方共同规划。各级政府官员和私营部门的代表应该不断地交流，确保对于彼此的关注事项、要求和期望的共同理解。政府不能直接强迫私营部门的参与和遵从，不论是依靠法律手段还是规章条例。更重要的，合作关系意味着政府决不能做任何有损于公民自由的事情。

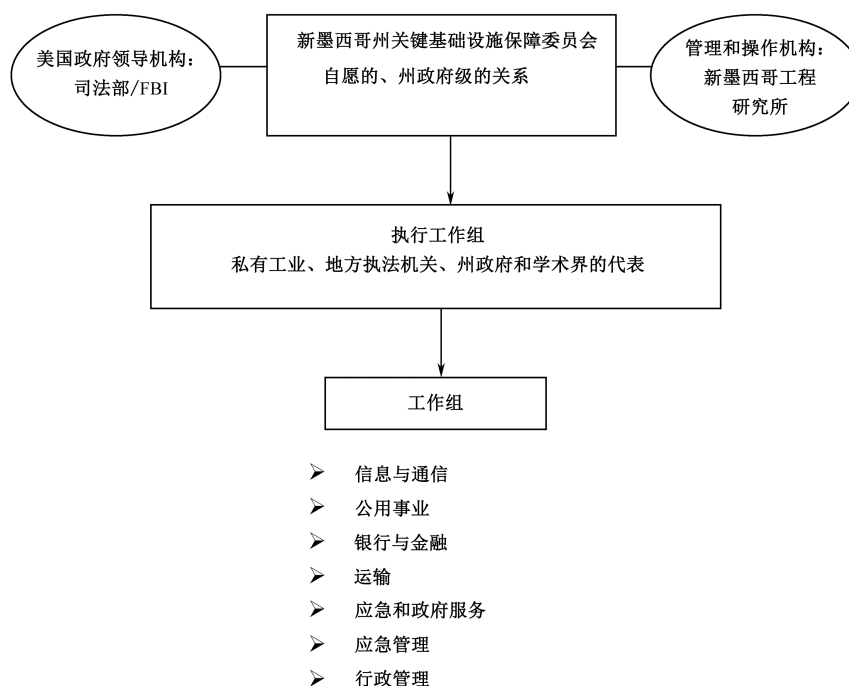
这种合作关系将促使举国努力来保护我们的关键基础设施。故而在这里并没有提出明确的计划，本章只是建立合作关系的框架，概述联邦政府应如何帮助并鼓励公共-私营合作关系的发展。因此，本章把私营部门和州及地方政府划到了一起，虽然我们知道它们之间其实有着明显的不同。如果我们的工作能够取得初步的成功，那么，在后续版本中的本章将不会只限于描述一般性框架，而是给出一系列由工业界和各级政府都共同首肯的特别行动和项目。

### 州及地方政府的角色

州及地方政府处在保护关键基础设施、抵御有意攻击的前线。它们均拥有并操作着一定的基础设施，并同私营部门的基础设施有着物理上的邻近以及最为紧密的交流。因此，CIP工作把州和地方政府看作一个独立的部门。

在千年虫防御中，州及地方政府同私营部门并肩战斗过，有些地方政府和私营部门甚至已为处理长期的关键基础设施保护事项建立了合作。在执法和其他领域，联邦政府同各级地方政府的合作关系由来已久，目前联邦政府正努力增强并扩展这些必要的合作，并在这些实体和私营部门间也发展这种合作关系。

至少在一个州——新墨西哥州内，工业界、学术界和政府机构已经自愿行动起来，组成了新墨西哥州关键基础设施保障委员会（NMCIAC）（见下图）来保护该州的关键基础设施，防御物理和计算机威胁：





本章贯穿始终都在讨论州及地方政府和私营部门在保护国家的关键基础设施时的相互交流和作用。在本篇国家计划的后续版本中，我们会用独立的章节来介绍私营部门、州及地方政府同联邦政府合作来保护我们国家的关键基础设施的各种工作。

### **私营工业的角色**

对私营工业来说，计算机安全会给它们业务的成功乃至整个私营工业的生存产生直接的影响。私营公司知道，它们必须为其客户，不论是公共还是私营的维持稳健而可靠的服务提供系统。为了树立客户的信心并在激烈竞争的市场环境中生存，很多成功的公司已经施行了很多项目，以保障系统和操作在遭破坏时其业务仍能正常开展。而对信息技术日益增长的依赖以及技术应用时带来的新的威胁和脆弱性则为这些保障工作增加了新的内容。

美国商业领导一直就有着组织工业力量、为国家挑战出谋划策的历史传统。他们在完成这些事情时，其行为同国家利益是一致的。但是，他们并不是利他主义者，他们这样做的原因是为了确保其业务的可靠性，只不过这时国家利益和这些股东的利益一致罢了。

这方面的例子包括北美电力可靠性委员会（NERC）以及国家安全电信顾问委员会（NSTAC）。前者的重心在国家的电力网，后者则致力于与美国电信网络有关的国家安全问题。它们是那些既服务于客户也服务于公共需求的工业委员会的榜样。它们均含有公共的主题，那就是保障其各自系统的可靠性、可用性和完整性。

### **国家安全电信顾问委员会（NSTAC）**

- NSTAC 是一个总统顾问委员会，建立于 1982 年 9 月，用以向总统提供专家建议。
- NSTAC 由多达 30 个的工业界电信代表公司的高级领导组成。
- NSTAC 组成了各个子工作组来分析与通信有关的国家安全和应急准备事务。
- NSTAC 与国家通信系统（NCS）密切合作，是工业/政府联合计划制定时的焦点。

### **北美电力可靠性委员会（NERC）**

- 由 10 个地区级的可靠性委员会组成，目的是非盈利的。
- 涉及了整个电力工业的所有部分，包括私营部门所属的公司以及州、地方和联邦政府的公司。
- 实际负责美国和加拿大的所有电力以及墨西哥的部分电力。
- 吸取各种经验教训、监督对政策、标准、原则和指导的遵循、评估电力系统的性能，从而促进北美电力系统的可靠性。

### **2000 年问题以及工业界和州及地方政府的角色**

有些时候，私营部门是公共威胁防御中公共-私营合作的催化剂。在千年虫防御的初期，很多公众和工业界人士认为千年虫事件的急迫性还没有得到充分的重视，他们敦促政府来提高意识并加速行动。于是，联邦政府在现行工作的基础上立刻开展了促进合作关系的活动。虽然在对各种成功和不足进行全面研究后，我们还只能看到这些工作的部分有效性，但我们确实相信，是这种改良后的公共-私营合作关系使得千年虫问题变得可控。

千年虫事件第一次测试了信息时代的国家基础设施保障项目。千年虫将会带来的可能的系统故障要求基础设施的所有者和操作者的保障项目中包含重建计划，联邦政府的角色是保障私营部门和州及地方政府的各类项目能够在国家范围内得到协调和有效执行。

从千年虫事件防御工作中得到的经验关系到信息安全的公共-私营合作。为了在服务 and 产品保障项目中利用这些经验信息，任何工业和公司要做到：

- 评估关键业务操作对信息技术的依赖性；
- 评审当信息流遭到破坏时对业务操作和客户关系带来的冲击与后果；
- 评价公司风险轮廓的变化，努力采取各种必要的矫正性措施来确保服务或产品能够达到客户和公众的期望；
- 继续评价未来的信息技术投资，在关键业务操作中考虑进安全风险。

企业领导人意识到，他们各自公司的蓬勃发展将会受到整个工业界发展的影响。所以，这些本质上为了业务管理运行的行动，也同样可以作为保护国家安全、防御各种威胁以及保障工业界经济利益的手段。

### 为实现公共-私营合作关系的联邦组织

白宫和一些关键的联邦机构正直接同主要的私营部门和州及地方政府的领导者和组织者合作，共同制定本篇国家计划。根据 PDD63 以及后续的决定令，联邦领导机构正接受委派，同各自针对的基础设施部门合作，对其组织进行支持。在过去的几年中，很多基础设施部门已经指派了部门协调机关，支持了相应的联邦领导机构，具体见下表：

关键基础设施部门	私营部门协调机关	联邦领导机构和部门联络官
信息与通信	美国信息技术协会； 电信工业协会； 美国电话协会	商务部 Greg Rohde，通信和信息助理部长
银行与金融	银行与金融协调委员会	财政部 Greg Baer，助理副部长
供水	大城市水工业协会	环保局 J. Charles Fox，水事务办公室助理行政官
航空、高速公路（包括汽车运输和智能传输系统）、大宗运输、输油管、铁路以及水运贸易	（待定）	交通部 Rear Admiral Bert Kinghorn， 情报和安全办公室主任
应急执法服务	州及地方政府执法委员会	司法部/FBI Michael Vatis，NIPC 主任
消防应急服务 政府服务连续性	州消防队长国家协会	联邦应急管理局 Denis Oniea，国家火灾学会主管；Catherine Light，国家安全事务办公室主任
公众健康服务	（待定）	健康和公众服务部 John Callahan，助理部长
联邦部门	（不适用）	总务管理局 Thomas Burke，信息安全办公室助理委员
电力、石油和天然气生产及存储	北美电力可靠性委员会； 国家石油委员会	能源部 General (Ret.) Eugene E. Habiger，安全和应急操作办公室主任

联邦政府和私营工业经过努力合作，已经在每个部门内都开放了关键基础设施保护的对话。

- 1998 年 11 月，由能源部、天然气研究学会、电力研究学会（EPRI）发起的能源论坛得到了超过 100 个的电力工业、石油和天然气工业以及政府代表的参加。1999 年 4 月，在得克萨斯州的哈斯顿成立了第二个能源论坛，由 EPRI 发起的第 3 个论坛于 1999 年 11 月成立，参加代表达到了 150 个。

- 通过部门协调委员会，银行与金融业已经开过几次碰头会，制定了相应的计划以解决风险评估、工业信息共享、研发日程以及向工业部门领导层的推广等问题。

#### 银行业技术秘书处<sup>①</sup>

为推动电子银行和电子商务的安全性和稳固性而建立的金融服务安全实验室及测试过程

银行业技术秘书处（BITS）是为金融服务圆桌会议而成立的技术组织，它支持开放环境中的电子银行和电子商务的成长和发展，鼓励金融机构及其客户更多、更有效地使用金融软件、访问工具、网络以及电子处理设备。BITS 将推动支付系统和电子银行的产品安全性和稳固性，它的董事会成员包括 14 个美国最大的银行股东公司的主席或首席执行官（CEO）、美国银行家协会（ABA）的代表以及美国独立银行家协会（ICBA）的代表。

最近，BITS 宣布其金融服务安全实验室的成立。该实验室由各个参与方的资助，一个致力于信息保护、电子商务安全以及信息工程系统的私营咨询公司进行运行。其主要关注对象是：

- 早期产品影响（Early Product Influence）；
- 风险减缓（Risk Reduction）；
- 成本缩减（Cost Reduction）；
- 安全功能（Security Functionality）。

安全实验室将最终对产品性能进行测试，检验它们是否满足了与安全属性有关的专门标准，这些属性包括认证、完整性、保密性、隐私、可追究性以及授权等。成功通过测试周期的产品将会得到一个“BITS-tested（BITS 测试）”标记，标明了该产品的整体安全水平。在 BITS 的网站上可以看到这一标记。

1999 年 10 月 1 日，美国财政部长宣布成立银行与金融服务信息安全设施——金融服务信息共享和分析中心（FS/ISAC）。

FS/ISAC 是公共-私营联合努力的结果，旨在当金融服务业受到计算机威胁时将其受害的消息进行共享。它提供了匿名式快速传播威胁消息的手段，从而加强了工业界阻止、检测和响应那些针对其技术设施的攻击行为的能力。

所有经认可的金融服务协会的会员均可以获得 FS/ISAC 的成员资格。当前，12 个分别代表公共和私营利益的组织已经签署了加入该中心的确认函。该中心由一个私营的承包商来管理，经费则完全由各参与会员提供。

联邦政府已经制定了有关计划来发展同州及地方政府的必要关系。通过与各个组织，如国家州长协会、美国市长会议以及已开始制定其关键基础设施保护项目的各个州及地方政府的合作，联邦政府正鼓励他们帮助在政府和私营工业之间建立起重要的合作关系，以保护国家的基础设施，防止处心积虑的攻击。比如，各州及地方执法机关已经指派了它们的部门协调地和部门协调员，并完成了最初的行动计划草案。

还有其他一些类似活动也正在开展之中。国家协调员和联邦其他高级官员正积极对话，以解决跨部门的关心议题。很多追求利润最大化的公司已经意识到了这方面的市场，并为了组织信息系统保护而开展了同私营工业客户的合作。

<sup>①</sup> 详细信息见 BITS 的网站 [www.bitsinfo.org](http://www.bitsinfo.org)。——译者注

### 对私营部门和州及地方政府关键基础设施进行保护和防御的行动

随着对关键基础设施保护需求的认识的不断加深，大多数商业人士将问到的第一个问题会是：“这将对我的业务产生怎样的影响？”。

只靠联邦政府是无法回答这一问题的。通过公共-私营合作关系以及与州和地方政府的协作，我们也许可以得到一些详尽的答案。然而，即使在现在这样的初期阶段，我们也建议私营部门和州及地方政府要考虑参与本篇计划中的一些项目性活动，包括确定并矫正脆弱性（内容 1），组织对脆弱性、威胁和攻击信息的共享中心（内容 4），对研发项目投资（内容 6），增强工业界对于改进计算机安全需求的认识（内容 8）。

#### （1）标识关键基础设施资产和公共的互依赖性，查找脆弱性（内容 1）

联邦政府号召对工业界的基础设施保障计划进行周期性的不断评估，尤其要关注信息系统、工业机构和最佳实践措施的作用以及工业界对它们的依赖。

很多工业部门已经开展了风险评估并采取了矫正措施，为了向其客户和公众负责，它们已经建立了内部响应机制。联邦政府正在收集、分析和研究同计算机安全技术、操作和趋势相关的大量信息，而这些领域正是私营工业可以涉足的。审计总署的报告《信息安全管理：向领先机构学习》就是一例。能够交流的信息理应得到交流，适当的双向交流和支持性的合作关系应当在州及地方政府建立起来。

联邦政府还将为部门的风险分析提供支持，各机构已经筹备了必要的专家资源。在合适的时候，联邦政府将向私营工业和州及地方政府实体明确并提供这些资源的使用，以帮助它们完成风险评估。比如，总务管理局（GSA）和关键基础设施保障办公室（CIAO）已经筹备了“脆弱性分析框架”，正广泛用于各部的关键基础设施保护计划的制定。该框架或其他类似的框架也可以促进私营工业和州及地方政府的工作。另外，FBI 正在编纂每一部门的关键基础设施提供商列表，其各个区域办公室正着手建立同这些提供商之间的合作。

除了执行风险评估工作外，私营工业尤其可以在如下两类关键活动中担当领头羊的角色：

- 共享并推动操作建议：需要为信息系统安全制定并发展符合标准的且有效的定义，并使其在商业领域能够共享。从传统上来说，工业界在发展并确定操作建议和标准的任务中扮演着定义者的角色。联邦政府有时候也委托外部机构来制定标准和备案过程。当然，当市场自身的步伐不能满足用户的需求时，联邦政府将作为催化剂参与到其中。
- 引入相关的风险管理，使信息系统安全成为业务运行的一个合理部分：信息技术已经在很多核心业务的处理中得到了应用，但如果没有充分的管理控制和系统安全，就同时也意味着新的风险。商业运行对于信息系统的日益增长的依赖性必然意味着信息系统安全要成为谨慎的管理控制和操作的一部分。很多从事审计和风险管理职业的人在评估其公司、机构以及客户的风险时是深谙此理的。随着我们对千年虫事件的关心，更多人也明白了这一道理。在很多公司和州及地方机构内，这些专家负责把同风险有关的事项直接报告给高级管理层。通过与这些专家交流应急处理以及相关的国家议程，在一般商业和地方以及州团体内，人们的意识将得到全面的提高。这些意识以及对威胁信息、工具、技术、资源、操作和工业界标准的共享将提高他们对其职务风险进行确定及交流的能力。

#### （2）组织起有关脆弱性、威胁和攻击信息的共享

PDD63 建议在同联邦政府的协作下，私营部门要建立起信息共享和分析中心（ISAC），以促进关于脆弱性、威胁、入侵和异常现象的信息共享。这些中心可以为工业界以及必要时为 NIPC 提供私营部门信息的收集、分析、合理过滤以及传播。它们还可以为私营部门收集、分析和传播从 NIPC 来的信息。各 ISAC 可以作为优秀分析中心，为各种基础设施建立基本统计信息和模式，还可以成为各部门的信息交换地。而且，它还能够存储大量的历史数据以供私营部门使用或用作 ISAC 或政府认可的其他合适用途。

各私营工业将自己决定是否加入 ISAC 以及这些 ISAC 应采取何种形式。国家协调员和联邦领导机构将担当起部门联络者，协调联邦政府现有的援助力量，通过各种活动，如论坛、启动基金以及物理设备等来响应私营部门的各种要求。联邦政府还将通过与部门联络官和国家协调员协商，帮助制定 NIPC 和 ISAC 之间的信息共享标准。在过渡期，联邦政府鼓励各部门内部以及部门间利用现有的组织，如 InfraGard 章程和各 CERT 来实现更好地通信。

为了鼓励私营部门 ISAC 的创建，人们曾做了大量的工作。1999 年 1 月，关键基础设施保障办公室（CIAO）发起了一次超过 70 个私营部门、州及地方政府的官员参加的会议，共同讨论了为促进信息共享而将采取的后续必要手段。

联邦政府正在发展国家范围内的入侵检测功能，既用于国防，也用于民事核心信息系统，以提供实时的威胁、攻击和脆弱性警报。通过计算机应急响应小组（CERT）以及各部的计划，联邦政府还将其信息采集与分析力量集中到了基础设施安全事务上。这些活动均可以使政府更好地理解其信息系统中的威胁和脆弱性。同样，私营部门和州及地方政府也应充分地利用这些成果和经验。

#### 计算机应急响应小组/协调中心

如果你的计算机网络被一种新的病毒攻击了，你将向谁求助？卡内基·梅隆（Carnegie Mellon）大学软件工程研究所的计算机应急响应小组协调中心（CERT/CC）将提供准确、及时的信息来帮助你解决计算机安全事件。

1998 年，CERT/CC 收到了向其报告计算机安全事件或求助的 41 871 封电子邮件以及 1 001 个热线电话。在这段时间内，它还收到了 262 份脆弱性报告，并处理了 3 734 起计算机安全事件——这些事件殃及了多达 18 990 个网站。

当安全脆弱性出现时，CERT/CC 的事件响应人员将帮助受感染的网站确定并矫正系统中出现的问题，制定系统防护和安全策略。它还将与受到同样事件感染的其他网站进行协调，并且当受害网站提出强烈要求时，它可以帮助同执法和调查机关的交流。

CERT/CC 同技术开发商和销售商密切合作，共同分析其收到的报告，以发现其中可能的系统脆弱性。它还向厂商提出必要的建议，从而减少产品中的安全脆弱性。另外，它将帮助解决各种问题，促进矫正方案向其他响应组和更大规模的 Internet 社区传播。

这些可以被私营部门和州及地方政府所利用的成果包括各种情报共同体的信息。能够确定新的威胁或意识到威胁的变化将有助于使资金投入到的最需要的地方，更好地利用最终资源，使其服务于政府和工业。国家协调员以及 NIPC、情报共同体、联邦执法机构正制定相关步骤，向主要的私营部门和州及地方州府决策者进行定期的威胁和脆弱性情况通报。这将有助于非联邦实体在评估风险时做出理智的判断并采取必要的矫正措施。

作为 ISAC 榜样的灾难控制和预防中心（CDC）

- 基于需求以及自愿的组织结构。
- 技术关注点以及专门技术特点。
  - 非指令性和非执法性职能；
  - 建立基本统计分析数据，明确各类基础设施的模式；
  - 信息交换地。
- 公共-私营合作性质，有联邦政府、州及地方政府的参与。
- 分散式管理。
- 多种功能。
  - 共享实时事件数据以及简报和脆弱性信息；
  - 多类共享途径，可以保护信息的保密性，防止因共享而导致的信息泄露。

（3）在研发上投资（内容 6）

导致信息安全系统不能更广泛应用的原因之一是对其购买、操作和维护的高费用。而政府在信息安全应用性研究和开发上的投资的加大将刺激这一市场的发展，使其提供更优更廉价的工具，尤其是在市场本身无法做到这一点时。信息安全工具性价比的提高将有助于其应用和普及的拓宽。

然而这些还不够。在完成国家基础设施评估后，国家协调员以及国家领导机构将为总统和国会制定必要的建议，通过使用各种激励政策，如税收、直接津贴和保险业要求等来推动私营部门在研发领域的投入。

（4）加强推广，使美国人意识到加强计算机安全的必要（内容 8）

关键基础设施安全合作组织项目将集中关注国家关键基础设施保护的强烈交流需求，强调了工业界和政府应如何合作来共同确保这些基础设施的安全。

合作组织将探究各种途径，使工业界和政府能够实现密切合作，从而减弱国家关键基础设施面临的威胁。为此，该项目将发起一系列有工业界和政府的首脑参加的研讨、会议以及工作组，以实现下列目的：

- 促进基础设施的所有者和操作者、风险管理集团、一般商业集团、州及地方政府乃至美国民众对信息安全的意识和理解。
- 使工业界能够在未来为国家计划贡献其力量。
- 确定并解决双方共同关心的问题，包括但不限于信息共享处理、法律和法规改革、标准和最佳实践措施的制定、教育和培训、研发活动等。

合作组织的开展将基于：开放和自愿的成员资格；共同的信任；经常性的交流；对彼此价值、期望、要求、关注事项和各自目的的充分理解以及清晰而集中的最终目标。

- 关键基础设施部门的集中推广和意识培养项目：通过各指定领导机构，联邦政府正开展一系列会议以及简报通告等活动，使关键基础设施部门的各个成员知晓信息安全的重要性与紧迫性。要使大家积极参与关键基础设施保护计划的制定并投入到保护工作之中，前提就是提高大家对信息安全的意识与理解。领导机构的部门联络官将帮助确定私营部门的协调员并与之展开密切合作，联合发起一系列白宫会议以及其他的各类工作组。
- NIAC：通过与相应政府实体的协商，国家协调员将建立起国家基础设施保障委员会（NIAC）。它是总统的一个咨询委员会，展现了政府同工业界合作的决心。该委

员会由多达 30 个工业界和州及地方政府的官员组成，这些人均由联邦领导机构或部门协调中心任命。NIAC 的成立使那些股东得以有机会向总统直接提交基础设施保障政策建议。

(5) 为联合行动确保稳固的法律基础（内容 9）

为了支持公共-私营合作关系，当局正同商业界、州及地方政府以及所有的美国人密切合作，以评审现有的法律和法规并提出立法议程。迄今为止，在同私营工业和州及地方政府讨论的基础上，立法议程包括了如下要素：

- 减少法律障碍，促进信息的有效共享：使有关在各企业之间以及企业和政府之间实现信息共享的法律事务变得明朗。在立法议程中，政府将解决保密性、反托拉斯以及责任等问题，从而在公共和私营部门间建立起信任关系。

司法部将为之定义各种必要的环境，使工业界可以发展两种机制来共享信息：业务评审函和司法部指南。两种机制均概述了共享的方式、内容以及其他专门事项。

在同各州政府的合作下，联邦政府将确定那些不利于国家计划中的任务执行的州法律。通过与很多关键代表，如全美检查长协会的讨论，将制定出覆盖信息共享责任诸问题的榜样（model）规则并提交给各州进行研究。要想协调各种责任解决方案，离不开关键基础设施合作关系中各方成员的参与。每个州都有其自己的法律管理责任，而对这些法律进行解释和使用的法庭决策则又新的层面上增加了法律的复杂度。因此，法律改革措施必须要融入私营部门和各州以及联邦政府的多方关心和考虑。

- 通过司法系统有效地惩办基础设施案件中的罪犯：提供威慑基础设施犯罪的法律力量，更加合理地对基础设施攻击后果进行法律量刑。

政府正同美国判决委员会合作，确保《美国判决委员会指导方针》能够适用于基础设施攻击带来的破坏性后果。例如，将考虑一些攻击后果的严重性，如拒绝服务攻击的“下游”效果所导致的损失。政府还将鼓励判决委员会就关键基础设施保障诸问题同各州进行交流，通过州判决委员会或直接将其作为联邦司法培训联系的一部分。

- 计算机犯罪事件的国际民事赔偿：计算机攻击是没有国界的。当局认识到，现有的关于基础设施攻击的国际赔偿机制是不完善的，很多国家还没有对计算机入侵进行定罪和量刑。通过多边和双边协定以及其他机制，我们将努力实现计算机犯罪的国际民事赔偿。

法律改革将吸取已有研究的成果，如联邦贸易委员会对电子商务中类似问题的探索。另外，还将以很多现有机构，如世界贸易组织（WTO）为可能的参照模型。

- 雇主-雇员关系：要定义更加明晰的框架，使工业界能够防备内部人员的攻击。

国家关键基础设施更多的则是受到了来自内部人员攻击的威胁。关键基础设施保护总统委员会（PCCIP）的推广项目中就这一问题同私营部门的关键基础设施所有者和所有者、州及地方政府、联邦法律决策机关、隐私权保护提倡者展开了广泛的讨论。为了解决这一复杂问题，尤其是在雇员的工作岗位具有高度敏感性时，下一步的法律改革必须纳入各方面的意见以及调查和研究中的发现。我们必须意识到，一个内部人员其实也完全可以站在外部人员的立场上。我们的政府将号召专家们对涵盖雇主-雇员关系的州和联邦法律以及其他隐私法展开评审，研究怎样使法律能够最大程度地实现隐私保护，同时又不会过度损害某些雇主的安全要求。

- 对应急响应中各种要求和政府提议进行分类：我们应该减少法律管辖权中出现的混乱。内阁将评审联邦政府提出的各种要求给私营部门带来的混乱，它将把各种机构对工业的管辖权进行分类，尤其是在应急响应和出现危机时。内阁将努力确保在提交的任何新要求中不会出现重复现象。

#### 前瞻：私营部门、州及地方政府同以后的国家计划的关系

基于这一框架，联邦政府官员以及私营部门、州及地方政府代表能够制定出国家计划的下一版本。目前这篇国家计划已经为政府的行动指示了明确方向，我们希望以后版本中能包括供私营工业选择和执行的明确行动的列表。该列表将是在真正的公共-私营合作联盟的基础上进行协作式、自愿式的深思熟虑后的结果。

## 附录 A 主要的联邦 CIP 官员和联系方式

名 字	头 衔	机 构	联系方式
Richard A. Clarke	安全、基础设施保护和反恐怖主义国家协调员	国家安全委员会	202-456-9351
Jeffrey A. Hunker	关键基础设施高级主管 (Director)	国家安全委员会	202-456-9361
Michael Vatis	主任 (Director)	国家基础设施保护中心	202-324-0307
Art Money	指挥、通信控制和情报防御助理部长	国防部	703-695-0348
John S. Tritak	主任 (Director)	关键基础设施保障办公室	202-589-3200
Liz Verville	副主任	关键基础设施保障办公室	202-589-3200
Greg Rohde	信息与通信部门联络官	商务部	202-482-1840
Greg Baer	银行与金融部门联络官	财政部	202-622-2610
J. Charles Fox	供水部门联络官	环境保护局	202-260-5700
Rear Admiral Bert Kinghorn	航空、高速公路、大宗运输、输油管道、铁路、水运贸易部门联络官	交通部	202-366-6525
Denis Onieal	应急消防服务部门联络官	联邦应急管理局	301-447-1117
Catherine Light	政府服务连续性部门联络官	联邦应急管理局	202-646-2979
John Callahan	公共健康服务部门联络官	健康和公众服务部	202-690-6396
Thomas Burke	联邦部门的部门联络官	总务管理局	202-708-7000
General (Ret.) Eugene Habiger	电力、石油和天然气生产及存储部门联络官	能源部	202-586-5000

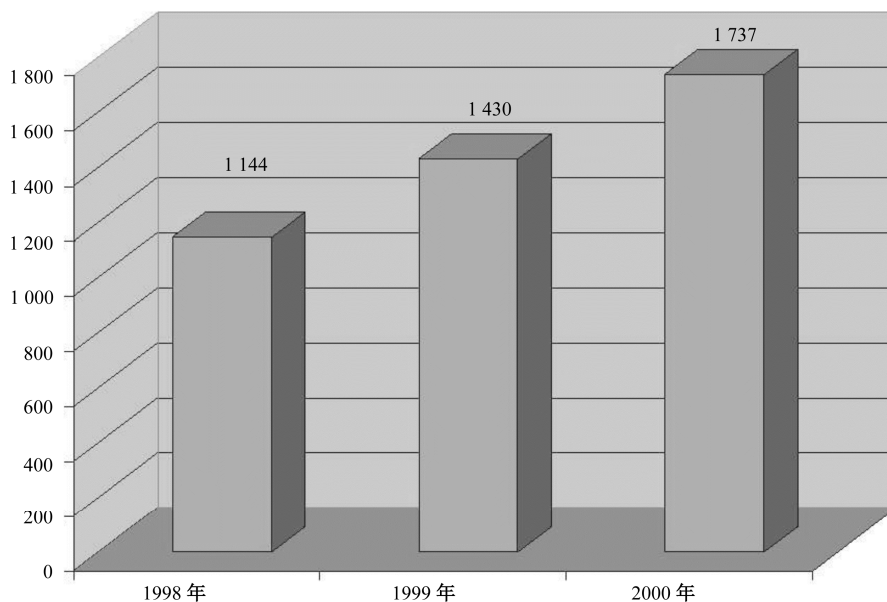
## 附录 B 预算趋势

### 概述

2000 年预算为政府范围内的基础设施保护提供了 17.37 亿美元。这比 1999 年增长了 3 亿美元，增幅为 20%。下图（单位：百万美元）显示了几几年的预算增长情况。这些预算一



部分用于新项目的开发，以解决主要的脆弱性问题，还有一些用于正在开展着的互联基础设施，如电信、银行与金融、能源、运输和关键的政府服务的保护工作（具体的数据可见后文的“对关键基础设施确定并拨款的跨机构过程”小节）：

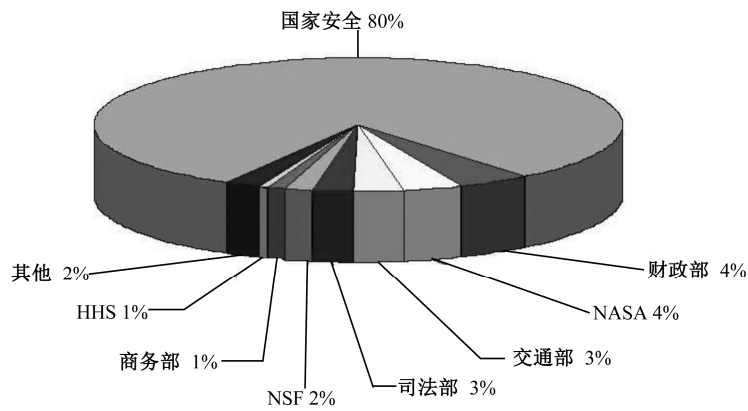


#### 各联邦机构在基础设施上的花销

几乎所有的行政部门的 CIP（关键基础设施保护）花销在 1998—1999 年之间都有增长。2000 年预算仍显示了这种趋势。这可以从下表（单位：百万美元）中看出：

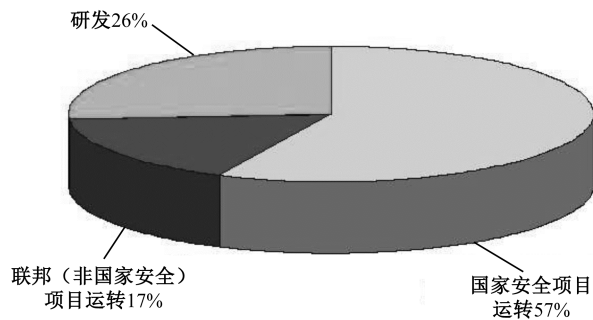
机构	1998 年实际拨款	1999 年实际拨款	2000 年预算拨款
国家安全	975	1 185	1 403
财政部	23	49	76
NASA	41	43	66
交通部	20	25	51
司法部	26	54	46
NSF	19	21	27
商务部	9	22	18
HHS	22	12	13
其他	9	18	37
总计	1 144	1 429	1 737

下图显示了政府各机构的关键基础设施保护拨款所占的比例：



项目运转和研发所占的关键基础设施花销比例

项目运转指关键基础设施保护中的常规基本措施。下图显示了项目运转（国家安全以及其他的联邦项目）和研发各自占的拨款比例：



由上图可见，CIP 花费可以分为项目运转（国家安全和其他联邦项目）和研发两部分。其中项目运转可以分为如下领域：

- 脆弱性评估；
- 风险管理；
- 保护和减缓措施；
- 入侵检测；
- 事件响应和事后重建；
- 教育和意识培养。

并非所有的机构都具有充足的数据来供我们对这些项目运转的预算数据进行特征化。但从今年开始，我们将认真收集数据并对其做出详细分析。

各行业部门的关键基础设施花销

下表列出了各行业部门关键基础设施保护的拨款情况，同时还列出了各部门间互依赖性的研究和相关活动所占用的拨款以及建立信息共享和分析中心（ISAC）所花费的拨款：

(单位: 百万美元)

关键基础设施	1998 年实际拨款	1999 年实际拨款	2000 年预算拨款
政府服务和应急服务	1 042	1 282	1 565
信息与通信	41	57	58
运输	25	32	57
电力、石油和天然气生产和储存、供水	22	35	30
银行与金融	12	17	15
互依赖性	2	7	5
ISAC	0	0	8
总计	1 144	1 429	1 737

下面将描述这些拨款在各关键基础设施部门、互操作性活动、ISAC 的运行情况。

- 政府服务和应急服务: 超过了上一年预算的 20%, 其中大部分都用于对国家国防机构的关键基础设施保护工作进行支持。
- 信息与通信: 3 300 万美元提供给了相关的 7 个机构, 用于计算机安全研究和制定有关提议。
- 运输: 针对联邦航空管理局的设施和信息系统, 并为了减少国家空间系统和地面运输系统中的脆弱性, 该部门的预算从 3 200 万美元激增到了 5 700 万美元。
- 电力、石油和天然气生产和储存、供水: 该部门在 2000 年的预算为 3 000 万美元, 用于支持能源部、内务部、环境保护局的那些现行项目, 使能源公司和大城市的供水机构能制定 CIP 计划。另外, 这 3 000 万美元拨款的其中一部分还将用于基础研究。所有这些工作均使我们朝公共-私营合作联盟的目标迈进了很多, 使公共-私营合作关系能够满足公共的 CIP 要求。
- 银行与金融: 财政部被划拨给了 1 600 万美元的预算, 用于协调银行与金融部门关键设施、关键设备以及操作的保护。根据总统令指示, 财政部要积极领导该关键基础设施部门的 CIP 工作, 同时还要成为其他关键基础设施部门的典范。
- 互依赖性: 联邦预算向国防部、商务部和国家科学基金会提供了 500 万美元拨款, 供它们研究关键基础设施间的相互关系, 使我们能够有能力确保这些互联的信息系统基础设施的可靠性和安全性。
- 信息共享和分析中心: 在 2000 年预算中, 部门联络官所在的各行业部门领导机构获得了 800 万美元的拨款, 用来协助信息共享和分析中心 (ISAC) 的建立。ISAC 旨在促进私营部门的发展, 共享各种操作建议和标准。

#### 新的和现行的关键基础设施活动

本小节讨论那些努力实现总统令中关键基础设施保护目标的具体活动。所列的活动有可能支持多个基础设施部门。这些活动仅仅代表了总额为 17.37 亿美元的 CIP 项目的一部分。

- 计算机安全研究和发展活动: 研发活动获得了 8 000 万美元的拨款, 以研究网络和数据库的保护以及异常行为、陷门、特洛伊木马和其他恶意代码的检测。

- 信息共享和分析中心：正如前面所言，ISAC 的设计是为了促进私营部门的发展并使私营部门共享操作建议和标准。为了帮助 ISAC 的建立，预算中为其划拨了 800 万美元。

除此之外，总统还将继续支持下列现行项目。

- 国家国防基础设施：联邦预算为保护国家安全所依赖的关键基础设施而增加了基金资源，使这部分的预算超过了 1.4 亿美元。
- 联邦航空管理和国家空间系统：为了更好地保护 FAA 设施和信息系统，并减少国家空间系统中的脆弱性，CIP 的 FAA 拨款翻了一番，从 2 300 万美元增加到 5 000 万美元。
- 打击计算机犯罪：联邦预算提供了 4 600 万美元用于加强 FBI、美国律师机关和司法部刑事处的调查及起诉工作。
- 关键基础设施保障办公室（CIAO）：CIAO 获得了 300 万美元用于支持国家基础设施保障计划的开发，这些拨款还将用于协调国家教育和意识培养项目。

#### 对关键基础设施确定并拨款的跨机构过程

自从 1998 年 PDD63 签署后，管理和预算办公室（OMB）就开始应其要求收集关键基础设施保护中的预算数据。虽然本附录中的预算数据显示了总统令发布后对关键基础设施保护工作的影响，并且这些数据的准确性达到了一定的程度，但在很多情况下，这些数据的质量还不能满足 OMB 的期望。

CIP 是一个较新的总统要求，机构的预算系统还不能及时支持 CIP 数据收集。因此，在这些预算系统做出修改之前，CIP 项目和预算信息的收集只能是手工式的，且很不准确。CIP 的新兴性还意味着政府仍处在“逆水行舟，不进则退”的学习和适应过程中，各机构仍需要对内紧抓其内部问题、对外积极参与跨机构活动。比如，对 CIP 的不甚熟悉影响到了各机构的设想的一致性，也造成他们所制定的相对优先级之间无法得到统一。上一年，OMB 第一次发布了 CIP 预算数据请求（BDR），以图搜集**行动级**信息。但因为各机构的行动描述不太充分以及数据表示方面的问题，OMB 无法融合这些数据，使我们难以确定项目中的重复和疏漏。这些重复和疏漏导致了不一致性的出现，从而不得不分析矫正。所有这些都减弱了数据的可信度。

为了解决这些问题，OMB 和国家安全委员会在去年春天开展了一项新的横跨各机构的优先国家安全项目评审活动。这些被评审的项目包括关键基础设施以及其他横向项目（即打击恐怖主义、大规模杀伤武器战备和运营连续性等）。横向性确保了这些项目的建议是在政府范围内做出的，而不是由一个个机构分别做出。评审活动涉及 4 个阶段。

- 项目评审：由国家安全委员会或科技政策办公室领导的各个跨机构工作组将在政府范围内评审各种与横向性有关的事项。各工作组将确定国家工作中出现的重复或空白，制定详细的项目活动，从而使我们能更加有效地对付非常规威胁。
- 预算评审：针对每一具体的横向领域，由各机构项目工作人员、各机构预算人员以及 OMB 检查官组成的预算子工作组将对项目活动的预算消耗进行估计。该阶段不会对各活动进行基金支持，而是要提供准确、公正的消耗估计。

- 各机构响应基金拨款建议：各工作组随后将对各个项目活动制定优先级，做出各项基金的建议并提供给联邦各机构。联邦机构将在综合考虑优先级的情况下研究这些基金建议，同时解决将向 OMB 提交的秋季预算中的有关财政问题。
- 机构响应行动的评审：OMB 将评审各机构对基金建议的响应行动，并基于工作组的信息、其他机构的优先级以及其他可用资源对其做出必要的改动。

这些旨在促进 CIP 数据收集和分析的工作在 2001 年总统预算提议中得到了明显的体现。该预算制定是在一个加速时间表下完成的（见下表），且 2002 年横向项目预算的制定也将依照该表。

CIP IWG（跨机构工作组）2001 年工作时间表

活 动	一 月	二 月	三 月	四 月	五 月	六 月	七 月	八 月	九 月	十 月	十一 月	十二 月
制定跨机构工作组的项目建议												
制定跨机构工作组的预算建议												
把 IWG 建议整合进机构预算中												
评审各机构对于建议的响应												
解决遗留问题												

这一时间表确保了各参与方都能有充足的时间确定其合理需求并确保各机构间没有出现项目断层或冗余。除了这一时间表之外，OMB 还要求项目和预算建议要符合一致的格式并提供足够多的细节，以便于预算分析。下面对项目评审样板做了描述。

- 项目描述：项目的内容，项目要买哪些东西或要做什么事情？
- 执行：哪个（些）机构将执行这些活动？
- 哪个（些）机构将为活动提供资金？解释这些选择的原因和基础。
- 背景：简述项目的历史，如果有的话，简述其他的类似项目。
- 基本原理：提供项目的理论推理。
- 同现有项目的关系：这是一个新的项目还是现行项目的增强？对于解决问题它是否采取了与以前不同的途径？
- 同多个相关总统令以及其他管理方针的关系：该项目是否是国家政策所要求的？它怎样支持了国家政策的要求？
- 同领导机构方针的关系：它怎样支持了领导机构对该类活动的指导方针？领导机构对其有需求吗？
- 同项目实施机构方针的关系：它和项目实施机构的机构任务以及战略性计划有什么样的关系？对该机构来说，它从事这一项目是否理智？该项目是否支持机构的脆弱性研究和威胁评估？
- 同私营部门的关系：这一项目为什么要由政府而不是私营部门实施？哪些数据显示政府有从事该项目的需求？相关的工业界是怎样看待政府在其角色的？
- 项目有效性：准备用哪种性能检验或评估方法对该项目的表现和有效性进行衡量？如何衡量？

预算评审样板如下所述：

- 项目描述：项目的内容，项目要买哪些东西或要做什么事情？
- 基金定位：注明将接受基金的机构/组织以及预算账户、预算账户明细表、项目管理办公室。
- 基金趋势
  - 项目的花费将为多少？是一次性花费还是连续性花费？
  - 对于那些现行项目，上一年度的基金投入是多少？注明所期望的国会对该项目上年度预算请求的反应。
- FTE（专职人员）趋势
  - 该项目还需要其他的专职人员（FTE）吗？需要多少？何种级别？
  - 对于那些现行项目来说，上一年度的 FTE 级别是怎样的？
- 基金资源提议
  - 上一年度的基础基金能否继续？
  - 能否对冲销或其他新的花费予以支持？

#### 关键基础设施拨款和项目信息的数据呼叫

跨机构评审的一个关键组成部分就是针对非常规威胁的年度 OMB 数据呼叫（data call）。数据呼叫中的信息将通知给跨机构工作组的项目和预算评审过程以及 OMB 的预算评审工作。为了完成数据呼叫，OMB 发布了预算数据请求（称为《对非常规威胁的国家安全剖析》），用于收集政府级的项目和预算信息。这些项目包括关键基础设施保护、反恐怖主义、大规模杀伤武器防御以及运营连续性等。收集来的数据用以判断各项目的资金需求是否得到了恰当的满足、确定政府各项目间存在的可能的断层、重叠和协同效果、监督白宫和国会感兴趣的特定项目的进展情况等。

现在数据呼叫可以利用数据库来收集行动级上的有关资金水平、注释描述和特征化等方面的信息。对预算中的每个有关活动来说，各机构应报告该活动在以前和当年的实际或预计资金花费以及未来年份中的基金请求。另外，各机构还要报告由 NSC（国家安全委员会）领导并负责评审这些项目的跨机构工作组所推荐的任何活动的基金情况。

## 附录 C 关键基础设施保护中的联邦研发日程

### 背景

在 PDD63 中，总统指示关键基础设施协调组（CICG）首脑委员会（Principals Committee）要在 180 天之内向其递交一份关键基础设施保障时间表，其中要有各任务日期的阶段安排。包括完成：

“研究和开发：由联邦发起的基础设施保护研发活动应当成为多年度计划制定时的主题之一，需要仔细协调；并且，联邦的研发活动还要对私营部门的研究做出重视。除此之外，研发活动的资金要得到充分的保障，以使我们在尽可能短的时间内把脆弱性降到最弱。”

为此，国家科学和技术委员会（NSTC）<sup>①</sup>下属的国家科学分委会和技术分委会以及在 PDD63 下成立的关键基础设施协调组联合通知 CIP IWG（关键基础设施保护跨机构工作组）制定联邦研究和开发战略，并使其成为更广泛的联邦关键基础设施保护（CIP）行动的一部分。这一战略强调了五个首要的研发议题，有三个对所有的关键基础设施部分来说是均需考虑的，分别为脆弱性和风险评估研究、信息保障研发、互依赖性分析；另外两个则更专门化一些，但也同样需要得到直接关注，分别是入侵检测和监控系统、自动化基础设施控制系统的安全。

IWG 定义了五个关键基础设施部门：银行与金融、信息与通信、能源、运输以及重要民生服务。另外，它还定义了一个综合研究领域，称为互依赖性。

要取得 PDD63 所要求的 2001 年初步目标以及 2003 年的全面目标，使美国具有并保持保护国家关键基础设施的能力，这看起来并不是一件容易的事。这种基础设施保护能力的保持将是一个动态的过程，因为伴随着技术的快速发展，新的脆弱性正不断地出现。现实地讲，2001 年初步目标的实现将主要依靠现有的技术，而 2003 年全面目标对新技术的依赖性充其量也只能到达一个有限的程度。然而，随着时间的发展，关键基础设施保护工作面临的挑战将只增不减。人性的特点、世界的多变，都使得我们的基础设施保护方案将总是处在与此相对的基础设施破坏的挑战之中。我们面临的将像《爱丽丝梦游仙境》中的一样，要尽最大可能地向前奔跑，跑在基础设施保护的最前方，而这种永恒的挑战则需要持续的研发努力来应付。

### 范围及目标

有效的联邦 CIP 研发项目应该能够增强我们国家的关键基础设施的安全性，快速确定、发展并促进针对现有和未来的基础设施威胁和脆弱性的技术解决方案的落实。为此，我们就完成下列事项：

- 要对新技术的发展在基础设施中的体现有所认识，还要意识到技术发展对这些基础设施造成的故意和非故意破坏。
- 要制定一个资金有保障的关键基础设施保护研发项目单（menu），使其能及时地用于政府及私营部门的资源分配和 CIP 的计划制定。
- 要建立同私营部门、学术界以及其他国家的有效的双向交流，使重复性研发的可能性降至最小，并确保在研项目能最理想地满足私营部门和政府的需求。
- 要有一个创新性的管理结构，该管理结构能够对快速变化的基础设施环境中的新技术和新威胁具有充分的灵活性并能做到足够的响应。

成功的研发项目将需要研究入侵检测系统，该系统在理论上要具有高检测率和低误警率。它还需要研究能够将基础设施的故障部分进行隔离并快速解决问题或迅速启动备份功能的系统，从而使基础设施的其他部分免于受害。但这还不能满足 PDD63 中的 2001 年和 2003 年目标。技术的不断发展使关键基础设施面临很多新的破坏方式，这要求必须要有持续的研发项目，使我们的关键基础设施始终保持稳健。跨机构工作组于是认为，为了实现 PDD63 的目标，离不开一个有效的关键基础设施保护研发日程表，这是至关重要的。

<sup>①</sup> NSTC 由克林顿政府根据 1993 年 11 月 23 日行政令成立。NSTC 及其下属委员会的详细资料可见于 [http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC\\_Home.html](http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html)。——译者注

基于 PDD63 的指示与国家安全以及技术分委会和关键基础设施协调组（CICG）的指导，跨机构工作组确立了如下目标。

- 在 PDD63 的方针下制定并协调联邦政府的关键基础设施保护研发日程：综合性的项目单将包括现行项目的信息、短期和长期研究计划的信息、预算信息以及研发政策提议。
- 监督并协调现行的和计划中的联邦 CIP 研发：跨机构工作组提供了一个论坛，用以确定并解决在推荐国家研发日程、研发政策和项目时遇到的诸问题。
- 为发展同私营部门、学术界和国际团体的密切合作关系而创造必要的条件：鉴于 CIP 研发项目中有很多要由工业界、学术界和国际团体完成，所需要的大量专家也来自于这些实体，联邦项目必须同这些实体联合开发、并结成密切的合作关系。
- 促进政府各机构之间以及政府和私营部门之间技术成果的迅速转让：在政府实验室中开发出的技术应该迅速转让给私营部门，尤其是在联邦政府专注于研究而私营部门专注于开发的情况下。
- 在合适的时候响应 NSC、国家协调员、CICG 以及其他基础设施保障部门的要求。

#### 各基础设施部门的研发要求

通过对已发现的以及潜在的基础设施脆弱性的审查以及对当前很多功能的分析，每一基础设施部门的研发要求已经得到了确定，如下所述。

##### （1）银行与金融

金融机构涉及了各方的利益，所以他们应该处在开发和使用安全方案的最前线。考虑到国家法令以及其他类型的核查在对金融系统，尤其是银行的控制中的显著角色，该部门时刻保持着警觉性，紧跟网络控制和安全工具的发展。私营部门在这一部门的安全研发中占据了主导地位，然而政府不但对整个美国金融系统的安全和完整性怀有浓厚的兴趣，而且还尤其关注那些政府拥有以及由政府运行的金融系统部分，如联邦储备委员会的 FedWire 支付系统。另外，金融系统的安全还要涉及执法和国家安全方面的严肃考虑，如对密码的关注等。

政府所关心的宏观脆弱性研究以及金融服务业内的现行基础设施安全研发要求可以分为如下几个基本领域：

- 认证技术；
- 物理和电子保护技术；
- 测试设备；
- 仿真模型的开发；
- 信息安全分析；
- 入侵显示和报警工具；
- 系统可靠性的增强；
- 信息系统标准化；
- 电子商务安全性的增强。

##### （2）信息与通信（I&C）

在这一美国经济关键部门中，我们要有新型的研发工作来解决不断出现的脆弱性。为此，如下九个领域需要引起特别的注意。



- I&C 基础设施的建模和仿真工具：将开发一套有代表性的建模仿真工具，用于开发和评估 I&C 关键基础设施保护技术。
- 脆弱性检测、评估分析：将确定、收集、组织并发布各个系统、网络和其他基础设施的脆弱性，并针对这些脆弱性开发应用技术，从而在软件开发以及系统集成时避免、减弱或消除这些脆弱性。
- 响应、恢复和重建：将开发用来控制、阻止或抵御入侵者的方法，并努力使破坏性得到减缓，或者在攻击、灾难性事件中恢复信息处理服务。
- 可靠性、生存力以及稳健性：将针对 I&C 基础设施研究应用技术，使网络的可靠性以及系统生存力得到增强，并确保基础设施中各系统和组件以及基础设施自身的稳健性。
- 风险管理和性能评测工具，安全测试方法和测量基准：将研究新的测量基准以及测试工具，如实时网络性能测量工具。
- 核心研究功能、基准测量流程以及操作建议：将开发 I&C 核心研究所要求的那些功能，并推动基准测量流程和操作建议在整个 I&C 基础设施间的使用。
- 安全体系结构：将在合适的体系结构下组织各组件/服务，为信息与通信系统提供保密性、完整性和可用性。
- 保障技术：将开发必要的工具和技术，用于软硬件组件以及后续集成的严格设计、执行、测试和检验。
- 入侵和事件检测及报警：将开发相应的工具和步骤，提供事件的检测、响应和恢复能力。这些工具将包括基于人工智能的系统，可以自动化地检测网络入侵的模式特征。

### （3）能源

美国的能源系统正变得日趋复杂，这将有可能对我们快速响应重大基础设施事故的能力造成削弱。下面列出的研究领域将既能对付现有的脆弱性，也可以处理随着能源工业的变动而出现的新的脆弱性：

- 脆弱性评估；
- 关键后果分析；
- 实时控制机制的开发；
- 高度安全性的 SCADA 系统的开发；
- 高效的可适应性加密的开发；
- 稳健的认证和授权机制的开发；
- 感应器和报警技术；
- 电能工业中的传输和配给系统；
- 应急响应和恢复步骤；
- 政策效果评估；
- 直接的能源技术；
- 规模和复杂度分析；
- 在线安全评估；
- 分散式能源产生（dispersed generation）；

- 决策支持系统;
- 对体制性 (institutional) 障碍的评估;
- 风险管理中的威胁评估。

#### (4) 运输

运输基础设施的主要组成部分, 包括各种模式的设施和物理、电子方面的内容应能经得住有意或自然性破坏, 并在破坏发生后要尽可能快地恢复到服务的正常状态, 这对于国计民生来说极为重要。虽然美国拥有世界上最好的运输和分配系统, 但他们对这些有意或自然破坏却并没有免疫力。交通部 (DOT) 正同私营部门、学术界、其他联邦机构、州和地方政府的用户和研究人员密切合作, 以确定广泛的安全要求并制定相应的项目来弥补这些安全缺陷。经过这些努力, DOT 已经制定了如下所列的研发活动列表, 并对 2000 年至 2005 年的相关安全活动的资金需求作了估计:

- 开发高度准确的惯性导航系统以及着陆备份系统, 用于在常规系统 (GPS、WAAS 和 LAAS) 崩溃时对飞机操作。
- 改进技术, 以对运输设备上发生的有毒化学和生物试剂泄露进行建模、检测并消除影响。
- 开发综合性的方案, 用于旅客和所有货运终端, 包括货物、设备、能源供应和电子及通信系统的安全性。
- 分别对比开放式和封闭式、分布式和集中式的运输操作系统模型, 分析脆弱性。
- 评估运输系统中人力因素的作用 (准备、预测和响应), 以决定未来的培训和教育需求。
- 评估智能传输系统和积极火车控制项目<sup>①</sup>中的电磁能力以及电子系统脆弱性。
- 评估 GPS 崩溃时对民事运输造成的冲击, 评估用于改善导航条件的国家差分 GPS 服务改良后的效果。

#### (5) 重要民生服务

供水部门的 CIP 研发要求曾经在总统关键基础设施保护委员会 (PCCIP) 的两篇报告 (《关键的基础: 保护美国的基础设施》和《关键基础设施保护和保障的首要研发指示》) 中阐明。其中的很多信息是由环境保护局 (EPA) 的工作人员提供的。

供水部门可能的研发主题和活动包括:

- 对生物和化学试剂进行确定并特征化;
- 开发针对生物和化学试剂检测手段;
- 实施 SCADA, 综合各种方式来阻止入侵和破坏;
- 开发供水系统的脆弱性评估工具;
- 建立供水系统风险评估优秀中心。

#### (6) 互依赖性

人们很早就意识到了基础设施之间的互联。早在 20 世纪 30 年代, 空军战术学校就开发了其“工业化网络”理论, 认为工业化国家的基础设施是互联的, 空袭者只要利用互联系统

---

① 积极火车控制项目与其说是一种技术或系统, 不如说是一种综合性概念, 它涉及数字通信、自动化定位系统等, 具有可降低事故发生率、减小运输损耗等特点。具体可见 DOT 的联邦铁路管理局网站 <http://framnd.volpe.dot.gov/html/ptc/fra-ptc.html>。

——译者注

的这些互依赖性，通过搜寻和攻击瓶颈——指可以造成敌方整个经济组织结构瘫痪的关键点，就可以达到攻击目的。如今，美国经济的互联性早已超过了半个世纪前的工业化时代。持续发展的计算机和信息技术使各个基础设施之间的互依赖性程度越来越高。我们现在是由多类基础设施组成的计算机化国家，对基础电信和信息网络组成的组织结构具有强烈的依赖性。同时，各种基础设施对国家的能源生产和分配网络也强烈依赖，尤其是信息与通信基础设施对能源有着高度要求。最终的结果是，我们的现代化基础设施紧密相连而融为一体，即使有时这种依赖性并不是直接和明显的。虽然我们约略知道一些这种基础设施互依赖链所带来的冲击和影响，但还没有对其形成全面的认识与了解。我们推荐了如下一些研究领域。

- 互依赖性特征化：将研究互依赖性的内容，对其特征化。
- 复杂度理论：基础设施是复杂的适应性系统，我们需要对美国基础设施的复杂和适应性行为进行研究。我们尤其需要知道基础设施在物理或计算机攻击时的现象以及性能下降的情况。
- 建模和仿真：如今，对巨大的互联且复杂的基础设施所进行的建模和仿真仍处于不成熟阶段。我们还需要拥有更加先进的模型，充分利用地方或国家基础设施实际数据以及物理网络布局和操作状态信息，来帮助我们发现关键的节点、紧急行为和脆弱性。
- 脆弱性研究：到目前为止，我们还对互依赖性还没有充分的认识，还不是很清楚互依赖性在国家基础设施中引入的脆弱性。因此，我们要仔细分析，以更好地认识脆弱性，发现关键节点和链接，制定相关策略来降低或消除这种脆弱性。
- 灾害减缓技术：在基础设施遭受攻击或出现其他故障时，采取如下响应是非常重要的：隔离受感染的基础设施部分，阻止破坏性的进一步扩散并修复破坏。这些步骤要求对基础设施链具有准确的把握，并掌握由这些互依赖性而引发的各种基础设施行为。
- 政策研究：由于基础设施之间的互联性，针对单独一个基础设施的政策有可能对其他基础设施产生难以预料的后果。对这种现象，我们还知之甚少，也不清楚怎样减小这种现象对基础设施整体带来冲击的可能性。

#### 开发联邦的研发项目单（R&D Menu）

联邦 CIP 研发跨机构工作组使用一种直接的方法来制定联邦政府的研发项目单。首先，跨机构工作组确定每一部门的主要脆弱性以及已得到政府资助的现行 CIP 研发工作和项目。其次，跨机构工作组设计出一套理想的、资金不受限的项目来解决这些脆弱性。这种理想项目与现实正在进行的工作之间的差距就构成了原始的材料，2000 年以及以后的研发项目单再依据这些原始材料制定。

##### （1）发展中的联邦综合性 CIP 研发项目单

鉴于技术发展的动态特征，在解决关键基础设施保护问题的完整项目单中，任何综合性项目都只能说具有暂时的意义。所有项目必须要在一个持续发展的基础上时时更新。目前 CIP 研发活动的综合性项目单中包含 71 个项目，包括：

- 银行与金融部门 9 个；
- 信息与通信部门 19 个；
- 能源部门 17 个；

- 交通部门 8 个；
- 重要民生服务部门 12 个；
- 互依赖性类中有 6 个。

这些项目中，有两个将不会开展，因为大规模破坏性武器保护组将在其自己的项目中对这些活动进行资助。这个列表是综合性的，但并不全面，所以各机构仍需继续探索新的研发领域。为了确保其实时性，各机构需要保持对研发项目单的时刻注意。跨机构工作组还认为，随着时间的发展，各个项目，包括将来制定的项目之间的相对优先级不能一成不变。

这些项目提议只是针对联邦政府的，没有直接提到私营部门正在开展的研发项目。联邦政府曾试图确定这些私营部门研发项目，但发现他们除了提供一些最一般性的描述外就不愿再透露任何情况了。

## （2）理解和认识项目单

对跨机构工作组确定的综合性项目列表的回顾有助于说明“计算机化国家”这一概念在美国关键基础设施中融入的深度和广度。在 71 个项目中，有 50 个（超过 2/3）是部分或全部用来解决与信息有关的问题的。而同计算机无关的项目只占不到 1/3，在整个综合性项目单中，它们占据的资金不到 20%。

通过对各机构活动的回顾，跨机构工作组还发现，有一些需求对大部分或所有基础设施部门来说都是共有的，如脆弱性和风险评估研究、信息保障以及互依赖性分析。

由于上述需求的横向特征以及其全面的重要性，这些项目应该在跨机构工作组确定的所有项目中具有最高的优先级。另外，跨机构工作组还认为有两个特别问题极为重要，必须给予立即注意，即入侵检测和监控系统以及自动化基础设施控制系统。

虽然针对入侵检测问题人们已经做了一些工作，但相对于期望达到的检测水平来说仍还不够。另外，政府在评审中发现，自动化基础设施控制系统，尤其是监督控制和数据采集系统（SCADA）对整个国家的经济举足轻重，但最近的研究却显示出这类系统的脆弱性非常突出。故而针对这两类问题的项目活动也理应得到优先重视。在所有的 71 个项目中，有 31 个涉及了上述几个优先要解决的问题。

- 脆弱性和风险评估研究：
  - 信息与通信部门脆弱性检测、评估和分析；
  - 信息与通信部门风险管理性能工具；
  - 信息与通信部门风险分析；
  - 能源部门脆弱性分析；
  - 能源部门风险管理中的威胁评估；
  - 运输系统脆弱性分析；
  - 空间基础设施脆弱性分析；
  - 交通部门中基于 GPS 系统的脆弱性评估；
  - 交通部门中一般系统对计算机攻击和 EMI（电磁干扰）的脆弱性分析；
  - 重要民生服务部门中供水系统脆弱性分析；
  - 重要民生服务部门中应急医疗服务系统的脆弱性分析；
  - 互依赖系统的互依赖性脆弱分析。

- 信息保障：
  - 银行与金融部门的认证技术；
  - 银行与金融部门的信息安全分析；
  - 银行与金融部门的电子商务安全性增强；
  - 信息与通信部门的保障技术；
  - 信息与通信部门的补丁应用检测；
  - 信息与通信部门的加密技术；
  - 能源部门的有效可适应性加密；
  - 能源部门的在线安全评估。
- 入侵检测和监控：
  - 银行与金融部门的入侵显示和预警（I&W）系统；
  - 信息与通信部门的入侵及事件检测和报警；
  - 信息与通信部门的人工智能陷门分析软件。
- 安全的自动化基础设施控制系统：
  - 信息与通信部门的安全管理控制和数据采集（SCADA）系统；
  - 能源部门的高度安全性 SCADA 系统。
- 互依赖性分析：
  - 互依赖性的确定和特征化；
  - 规模、复杂度和趋势分析；
  - 系统分析和仿真工具；
  - 后果分析和风险管理方法及工具；
  - 互依赖的系统的脆弱性评估；
  - 保护和减缓技术。

据估计，这 71 个项目的总拨款将达到 7.5 亿美元。这将使联邦 CIP 研发总花费在 1 年中增长 150%，因此显得难以实现，而且也未必有效。对这些大量的新项目拨款后，人们希望联邦政府不要经历通常的“助跑”过程，立刻投入到这些项目中。这么大的资金投入也许会立竿见影，但在目标的实现过程中可能会造成更加严重的资金投入浪费或无效。所有新项目的 6 年期拨款计划达到了 61.6 亿美元。

### 合作联盟

联邦政府面对着很多非常重要的 CIP 挑战，其中之一就是针对关键基础设施保护而建立并维持同私营部门、学术界和其他合适的国家的有效双向对话。在外流（outgoing）、单向的基础上建立合作关系并不难，事实上跨机构工作组已经向非联邦性质的很多组织做了大量有关的提议。但是，要建立真正双向对话却远不是那么容易。

在开发新的市场化产品和服务或解决内部问题方面，工业界资助的各种研发活动几乎是完全排外的。它们不愿意透露那些对他们意味着巨大经济利益的私有化产品和工作的任何细节，这是可以理解的。但这样做却对信息的交流带来了束缚，使得跨机构工作组也许只能简单描绘出工业界和工业界的相关投资机构 CIP 研发的大致情况。

## 研发调查

- 银行与金融：在银行与金融基础设施方面，还没有确定出私营部门做了哪些研究工作。虽然银行与金融工业已经对各类技术做到了有效利用，但跨机构工作组无法确定私营部门在未来是否将开发其自己的或参与开发保护国家级基础设施的新技术。
- 信息与通信：如今的公共电信基础设施包括了公共交换电信网络(PSTN)和 Internet。这两种独立的网络之间有着很多互依赖性，人们希望他们能够在未来有效地合并到一起。人们同样也希望，随着时间的发展，当我们期望的这种更加综合的电信基础设施形成时，PSTN 和 Internet 的独立研发之间的很多不同能得到淡化和统一。

当前，私营部门的研发集团正在研究将对 PSTN、Internet 以及这两种网络的合成系统的安全性造成影响的那些问题。具体如下所示（包括每一领域所影响的网络保障标准）。

- 专用网到网接口（PNNI）：稳定性、互操作性、生存力、政策和服务等问题；
  - 波分多路复用（WDM）：性能、服务质量（QoS）、安全和生存力等问题；
  - 无线：性能、可靠性、服务质量以及其他服务等问题；
  - 下一代 Internet（NGI）基础设施：性能、互操作性、服务质量、可伸缩性、生存力、政策和服务等问题；
  - 域间路由、政策路由/结构：稳定性、可用性、可靠性和政策等问题；
  - 标签交换技术：伸缩性、稳定性、服务质量、性能、互操作性、政策和服务等问题；
  - 主动网络：性能、安全、生存力以及服务等问题；
  - 服务质量、区分服务：性能、服务质量/服务等问题；
  - 多点传送：可伸缩性、稳定性、可靠性、安全性、政策以及服务等问题；
  - 操作和网络管理、分布式控制：伸缩性、稳定性、服务质量、性能、互操作性、可靠性、安全性、政策以及服务等问题；
  - 安全：安全性、生存力、性能、可伸缩性以及服务等问题。
- 能源：除了个别公司之外，从事 CIP 研发的主要非联邦组织为天然气研究院（GRI）、美国天然气协会（AGA）以及电力研究学会（EPRI）。它们在近年均经历了研发预算缩减的情况。跨机构工作组确实确定了私营部门关心的如下广阔领域，但是无法查明其中哪些非联邦赞助的研发活动目前正处于进行之中：
    - 分布式控制的操作和监控；
    - 大规模系统的分析和计算；
    - 高级控制方法；
    - 决策支持系统。

下面列出了能源部（DOE）确定的那些私营部门有可能感兴趣并参与的研发主题：

- 能源部门内的关键后果分析；
- 实时控制机制；
- 脆弱性评估；
- 高度安全性的 SCADA 系统；
- 有效的可适应性加密；
- 稳健的认证和授权；

- 感应和报警技术；
  - 传输和配给；
  - 应急响应和恢复；
  - 政策影响的评估；
  - 直接的能源技术；
  - 能源系统的规模度、复杂度分析；
  - 在线安全评估；
  - 分散式能源产生；
  - 决策支持系统；
  - 对制度性（institutional）障碍的评估；
  - 风险管理中的威胁评估。
- 重要民生服务：美国水工业研究基地是私营部门中对水工业问题进行研究的主要组织。各项目主要关注水质研究以及水质对公共健康和安全的影 响等。项目涉及广泛，从配给系统的理论模型研究，到各类污染物的化学和生物学研究以及物理保障措施的建立等，不一而足。其中包括：
- 配给系统的病原体入侵；
  - 配给系统和存储设施的水质建模；
  - 配给系统中氯腐蚀（chlorine decay）的特征化和建模；
  - 水中病原体的快速甄别；
  - 氯升压器系统的自动化反馈控制；
  - 饮用水中杯状病毒（caliciviruses）的检测；
  - 检测对人类有害的病毒的方法；
  - 饮用水中氯毒素的去除；
  - 水泄露检测。

对供水系统进行入侵的可能方法中涉及了监督控制和数据采集（SCADA）系统。很多组织，如 Tennessee Valley Authority、陆军中工兵兵种、垦务局均已将水工业 SCADA 系统和电力 SCADA 系统集成到了一起，并引入了部门互依赖性的内容。当前，对 SCADA 安全性的研究也是电子系统的重要关注对象。

#### 私营部门的研发费用趋势

我们可以得到自 1988 年起主要电信提供商在研发方面的费用。虽然在不同的提供商之间每年的研发费用波动巨大，但总的费用趋势显示出，从 1988 年到 1993 年，研发费用从 3.42 亿美元增加到了 3.76 亿美元，平均年增长率为 1.9%。然而，从 1994 年到 1996 年，这一数字从 2.72 亿美元锐减到了 2.19 亿美元，平均年缩减率达 7%。这种趋势令人忧心，尤其是在工业界的技术变革如此迅捷的情况下。

我们还有其他私营部门在电信研发方面投资的数据，虽然有些并不是非常全面。已公布的数据包括了如下电信公司的研发支出：Lucent（朗讯）、AT&T、Bellcore、Motorola（摩托罗拉）、Cisco（思科）、Alcatel（阿尔卡特）、Ericsson（爱立信）和 Nortel。这些公司的大多数是电信运营商（carrier）或销售商（vendor），并拥有大型的研发实验室。这八大公司的总贡献是很大的，远远超过了政府和电信服务提供商的贡献总和。虽然八大公司中最后三家不

是美国公司，但是它们都突出说明了私营部门的重大贡献，同时使我们从国际范畴的视野来强调电信领域的研发支出。

对这八大公司投资的数据研究则显示了另外一个令人不安的趋势：从 1985 年到 1995 年，八大公司的研发总成果大致增加了 64%，但其中五家美国公司的成果增长率仅仅是 50%。跨机构工作组故而强调，要对电信领域内的国外研发投资增长率远高于美国这一情况予以特别注意。

跨机构工作组还认为销售商的研发投资大于提供商的研发投资。在过去，人们为了基金资助以及创新性研发的需求而建立了贝尔实验室（现在名为 Bellcore），但如今其多年来的传统角色正迅速消失，转而代之为电信销售公司的那种角色。同销售商的研发投资有直接关系的是获利设备的售卖，因此有很大的易变性。

跨机构工作组已经开始筹备一系列的 CIP 研发工作组。考虑中的主题包括：对入侵检测进行研究，保障联邦的正常运行；改善政府-私营部门间的研发信息共享；国际推广；确保有足够多的受过培训的 CIP 研发人员，使人力因素在关键基础设施保护中发挥充分作用；等等。同时还考虑召开一系列讨论会。另外，跨机构工作组将同各工业协会（如 IEEE、计算机安全协会等）和咨询委员会[如国家安全电信顾问委员会（NSTAC）、总统信息技术咨询委员会（PITAC）等]以及其他机构建立进一步的联系。

#### 使 CIP 研发项目单得到更新

为了使 CIP 项目单始终具有时效性并与基础设施保护技术的趋势保持一致，有以下 13 个任务有待联邦政府去完成：

- 确定国家关键基础设施面临的那些可以采用技术手段弥补的威胁与脆弱性，并对确定结果做到时常更新。
- 确定联邦 CIP 的现行和提议的研发项目，并维持这一数据库，针对已知的私营部门、学术界的项目以及国际项目也按照同样的要求做。
- 开发并更新一个综合性的、概念性的研发项目单，用来解决已知和未知的基础设施脆弱性。
- 基于所制定的综合性项目以及所研究的脆弱性，确定现行项目更新时的不足和盲点。开发相应的标准来裁定联邦政府行动的优先级。
- 在受到日益关注的那些焦点问题上，与各界展开密切合作，包括政府部门及机构中的相关人员和部门联络官以及所推荐的各种研发力量。确定这些 CIP 研发项目单的预算要求，并协调每年度联邦预算周期内的这一活动。
- 为在政府内促进现行和计划 CIP 研发项目的信息共享，提供相关的论坛并制定有关提案。
- 促进联邦 CIP 研发与现有的联邦在其他领域内的研发项目之间的协调，避免出现项目重复或项目焦点的类似（如那些同大规模杀伤武器、高性能计算以及军事防护等有关的项目）。与其他跨机构论坛和工作组[如技术支持工作组（TSWG）和高性能计算等]在合适的地方进行协调。
- 促进联邦 CIP 研发同私营部门、州和地方政府、学术界以及国际项目之间的协调。



- 制定有关的提议，在政府机构内以及政府和私营部门之间推动技术的转让。（由于我们在谈到目标时曾对此多次提及，这句话显得有些多余。但是，对这项任务进行再次强调是非常必要的。）
- 建立并充分利用由外部工业界和学术界的关键基础设施保护研发学科专家组成的评审工作组，对各个现行和提议项目做出评审。
- 针对 CIP 研发，提出相应的机制来鼓励在政府、私营部门和学术界之间发展合作关系，并为其提供必要环境。
- 发展各种手段，协调在研发问题上向公众的推广。
- 注意可影响联邦项目的方向或有效性的国外项目 and 政策发展，考虑可能的有关国际协调。

### 管理挑战

鉴于这些提议研发项目的特征以及基础设施保障问题的规模和重要性，我们需要有创新性的管理概念和管理结构来运行联邦政府的这些 CIP 研发项目。下面谈到的因素说明了在有效制定并管理一个成功的研发项目单时，这种创新性管理概念和结构的必要性。

虽然政府将对主要的研究部分进行拨款，大量的开发工作仍离不开私营部门的活动。市场作用将驱动这类开发并指导其最终产生面向市场的产品。因为工业界要保护其私营项目和商业秘密，所以要实现联邦同私营部门在研项目之间的协调将是非常复杂的。要想在合适的时间完成合适的研究，使政府和私营部门的项目实现适当的同步化并确保政府开发的技术能及时地向工业界转化，就要求两者实现紧密协调和密切合作。

就其性质来说，政府的 CIP 研发项目单横跨了数目众多的联邦机构。为此，跨机构工作组要解决的重要问题就是确保机构内部单个项目之间的协调，更要使各跨机构的项目达成协议。同样，跨机构工作组还必须确保各类技术能够在各机构间以及向私营部门快速转让。到目前为止，跨机构工作组已经观察到了一些案例，在这些案例中，那些机构虽然确定了其研发需求，却全然不知它们所确定的项目在联邦政府的其他地方早就开始做了。还有，有时一个相似或相关的项目由不止一个的联邦政府工作组管理，如技术支持工作组和大规模杀伤武器保护跨机构工作组。于是，确保各小组之间的适当的协调和通信就显得异常重要。关键基础设施保护研发预算的横向特征更进一步加重了项目管理的复杂化，也同时显示了对创新性新式管理方法的需求。

技术、脆弱性以及威胁均在加速发展，这很快使得传统上的那种冗长的联邦预算过程已经跟不上它们加速发展的步伐。某年度内对脆弱性的技术矫正有可能过几年甚至几个月后就会变得过时。然后，我们将不得不发展全新的系统，而全新的系统又将带来新一轮的脆弱性。政府预算周期是 3 年（第一年制定，第二年在国会通过机构拨款法，最后一年项目开始执行），故而关键基础设施技术革新的高速步伐将迫使我们的系统要能够制定并协调政府范围内的研发项目。联邦的研发项目单必须具有灵活性，以适应技术和威胁的迅速变化。

联邦的研发项目应同州和地方政府进行协调。特别是我们需要紧急事件中的“第一响应者”和其他的协助人员，这种需求决定了重要民生服务部门的很多研究的方向。如果要在项目单中考虑进这些需求因素，我们就必须拥有创新性的管理模式，并同州和地方政府结成合作关系。

关键基础设施事件的潜在后果促使我们在考虑问题时应超越普通的商业解决方式。我们的信息和电信系统遇到的每一个重大故障，不论其源头是否是恶意的，均有可能威胁到我们国家的经济基础，而由此带来的社会和政治余波则将会进一步加重这种破坏性。这就是经典风险管理在处理灾难性后果时遇到的问题。从 20 世纪 40 年代末到 80 年代，针对核武器将造成的潜在威胁后果，我们有了新型的管理方式。同样，在互联性日益增强的 21 世纪中，由横跨各基础设施的大型故障所引起的潜在后果向我们发出了警告，促使我们研究 CIP 领域内的研发管理新方式。

#### 几点观察

- 2000 年联邦 CIP 研发支出据估计会达到 5 亿美元。
- 决定 CIP 研发拨款的恰当水平时应考虑进新的预算活动，包括在大规模杀伤性武器和反恐怖主义方面的 PDD62 新活动以及信息技术活动等。
- 要确保学术机构能够从事于 CIP 领域的基础研究并培训大量的关键基础设施保护科学家和工程师。但在该过程中，我们却面临着潜在的问题，部分原因在于我们很难唤起私营部门的参与。为解决这一问题，我们需要采取针对的行动，如联邦信息技术服务或其他项目。
- 由于 CIP 研发所依赖的技术环境有着动态的特性，在开始的几年中，我们要对这些研究不断地评审并修改。
- 联邦各机构对 CIP 研发的管理将影响到他们对项目单中各项目执行的步伐。但在不同的联邦机构中，CIP 研发管理经验有着很大的不同，故而我们要意识到创新性研发管理解决方案以及研发监督的协调性对于 CIP 研发项目单的重要。
- 关键基础设施保护为冷战后的联邦管理系统提出了最迫切的要求。技术的快速变化使得未来的基础设施及其保护的风景线比起冷战时代来变化快得多，这种高速变化的步伐是一种双刃剑，在为我们带来利益的同时也使我们看到了各种敌意或非敌意破坏的可能性。
- 针对这些挑战，任何研发过程和活动必须具有足够的灵活性，以适应这种不断发展的技术环境。

#### 建议

- 在关键基础设施保护中，美国需要有数目众多的研发项目，从而确保当新的技术出现时，这些基础设施仍旧安全。
- 现行和计划中的 CIP 研发项目需要与总统倡议的其他活动相协调，促进各项目的协同效果，防止出现项目重叠。
- 在 2002 年的预算周期内，应提议一个相关项目来加强大学在 CIP 研发支持方面的培训和研究工作。
- 为了确保 CIP 研发能够与发展中的 CIP 技术环境同步，国家科技委员会应当为研发管理模型增加新的内容，使之具有灵活性。而且，在联邦政府内外，均要努力探索这种模型。

## 附录 D 术语表和缩略语

术 语 表

访问（Access）	进入或使用一个系统及其资源的权利；读、写、修改或删除数据的权利；使用软件进程或网络带宽的权利
报警（Alert）	把针对一个组织的信息系统所发动的攻击行为进行通报
异常检测（Anomaly Detection）	通过查看不同于用户或系统的常规表现的活动来检测入侵
保障（Assurance）	使对如下内容具有信心：系统设计满足了其要求或系统的执行能达到规范要求，或者特定的所有权要求得到了满足
攻击（Attack）	一个实体作用在另一个实体上的恶意行为，试图使另一实体遭到破坏或削弱其功能
攻击特征识别（Attack Signature Recognition）	用来识别已知攻击轮廓中可确定的特征（技术的、步骤的或基于设备的的）的方法
银行与金融（Banking and Finance）	一种以下列实体的活动为特征的关键基础设施：零售和商业组织、投资机构、交易所、国际贸易商行、储备系统以及相关的运行组织、政府操作和支持活动。该关键基础设施涉及了所有的货币交易，用途包括存储目的、收入再投资目的、薪金兑换目的、贷款以及其他金融手段的支出
能力（Capability）	经过适当组织、培训和装备的实体的功能，可以访问、渗透或改变政府或私营部门所属的信息或通信系统，和（或）使关键基础设施全部或部分遭到破坏、崩溃或瘫痪
首席信息官（Chief Information Officer）	机构官员，可以向机构的首脑或其他高级管理人员提供建议和其他帮助，以确保信息技术的获取和信息资源的管理都符合了国会制定的政策和步骤以及机构首脑建立的主要规定。CIO 是通过修正 1995 年《消减文书工作法》的第 33506 节后，应 1996 年《信息技术管理改革法》（ITMRA）的第 5225（a）节而建立的
公民自由（Civil Liberties）	宪法、自由法和联邦法律、法规所保护的权力和个人自由
竞争（Competition）	两个或多个实体相互算计以取得各自目标的行为。是“军备竞赛”的商业同义语
计算机应急响应小组/协调中心（CERT/CC）	是位于卡内基·梅隆大学的软件工程研究所的互联系统生存力项目的一部分。它关注和记录 Internet 攻击事件，并发布公告
计算机应急响应组（CERT）	由信息系统所有者特许的组织，针对威胁其信息系统可用性和完整性的计算机紧急事件采取协调并/或完成必要的响应行动
后果管理（Consequence Management）	包括保护公共健康和安全，恢复重要的政府服务以及向受到恐怖主义事态后果影响的政府、商业、个人提供应急救援。美国法律向各州授权对恐怖主义事态后果进行响应；联邦政府在需要时会提供帮助
危机管理（Crisis Management）	包括对用于预测、阻止和（或）解决恐怖主义威胁或行动的资源进行确定、获取以及制定使用计划。美国法律授权联邦政府来阻止和响应恐怖主义行为；各州和地方政府在需要时对其进行帮助。危机管理主要是执法性质的响应活动。基于具体情况，联邦风险管理响应可以得到技术操作和联邦后果管理的支持，后者往往是同后果管理一起执行的
关键基础设施（Critical Infrastructure）	对国家来说非常重要的那些系统和资产，既有物理的也有计算机的。它们非常重要，以至于其遇到的任何瘫痪或损毁将对国家安全、国家经济安全、和（或）国家公众健康和安全产生巨大的破坏性影响
网络攻击（Cyberattack）	利用基于信息技术的控制组件中的软件脆弱性而发动的攻击
网络空间（Cyberspace）	描述我们周围互联的计算机和社会的词汇。通常叫作互联网（Internet）
衰弱的（Debilitated）	国家安全或经济安全变成无效时的状态

续表

国防（也称国家安全） （Defense）	对如下内容的保证：国内外美国人的生活和个人安全得到了保护，美国的主权、政治自由以及独立，及其价值、制度以及疆域保持了完整
拒绝服务 （Denial of Service）	一种攻击形式，使资源变得不可用
毁坏（Destruction）	一种状态，此时关键基础设施失去了向其用户提供预期产品和服务的能力。这种状态主要指一种永久性的情况。当基础设施的性能指标变为零时就视为发生了这种情况
经济安全（也称全球经济竞争力） （Economic Security）	对如下内容的保证：国家的产品和服务可以在全球市场上成功参与竞争，维持或提高美国公民的实际收益
电力系统 （Electrical Power System）	以发电厂和传输及配电网络为特征的一种关键基础设施，可以为终端用户产生并提供电力，以使终端用户完成并维持其正常功能。电力系统还包括对电力产生非常重要的石油的传输和存储
应急服务 （Emergency Service）	以个人或社区在应急响应时依靠的医疗、警务、消防及营救系统和人员为特征的关键基础设施。这些服务通常在地方的级别上提供（县或城区级）。另外，州和联邦的响应计划均定义了协助响应和恢复的应急支持功能
专家评审组 （Expert Review Team）	由帮助政府实体开发内部基础设施保护计划的安全专家组成；ERT 负责通过共享操作建议、确保坚固的基础设施框架、确定技术资源需求，从而提高政府范围内的信息系统安全
防火墙（Firewall）	一种电子边界，可以阻止非授权的用户访问网络上的特定文件；一台具有这样的边界功能的计算机也称防火墙
天然气和石油的生产、存储和运输	以下列内容为特征的基础设施：天然气、原油和石油以及石油燃料的生产、保存设备；石油的提炼和处理设备；向依赖天然气和石油的系统运输这些资源的输油管、货船、货车、铁路系统
政府服务（Government Services）	联邦、州和地方级政府提供的满足公众重要服务需求的能力
失能，失去作用 （Incapacitation）	一种非正常状态，此时关键基础设施向其用户所提供的产品和服务的水平变得下降。该词指的是一种暂时状态。当持续的性能下降引起了系统的衰弱时，该基础设施就会被认为处在失能状态
信息与通信 （Information and Communication）	以计算机和电信设备、软件、进程和相关人员为特征的关键基础设施，它支持下述功能： （1）数据和信息的处理、存储和传输； （2）把数据转化为信息，把信息转化为知识； （3）数据和信息本身
信息保障 （Information Assurance）	通过确保可用性、完整性、鉴别、保密性和不可否认性，从而保护并防御信息和信息系统的信息操作，包括并入保护、检测和反应功能，为信息系统的恢复做准备
信息安全 （Information Security）	为了减少系统风险，尤其是减小被对方以电子、RF 或计算机手段成功攻击关键基础设施弱点的可能性而采取的行动
信息共享和分析中心 （ISAC）	私营部门建立的中心，服务于私营部门信息的收集、分析、适当过滤以及传播。这些中心还可以收集、分析并传播 NIPC 提供的信息，从而进一步向私营部门发布。ISAC 还用于共享关于脆弱性、威胁、入侵和异常的重要信息，但它并不干涉公司和政府间的直接信息交换
信息系统 （Information System）	用于信息收集、处理、存储、传输、展示、传播和处置的基础设施、组织、人员和各种组件的总称
信息技术 （Information Technology）	处理信息的硬件和软件，不论涉及的技术是计算机、电信还是其他方面

续表

基础设施 (Infrastructure)	互相依赖的网络和系统的框架,由可定义的工业、机构(包括人员和处理步骤)、分配功能模块所组成,提供对美国国防和经济安全至关重要的产品和服务,使各级政府和社会整个部分均保持功能的平稳
基础设施保障 (Infrastructure Assurance)	预备性和事后的风险管理活动,旨在使基础设施的性能水平在即使遇到了破坏性威胁时也能满足用户的预期需求,如事件减缓、事件响应、服务恢复等
基础设施保护 (Infrastructure Protection)	事前的风险管理活动,旨在防止对基础设施造成破坏或失能后果的行动或尝试,如威胁消除、脆弱性防护等
意图(Intent)	一系列有意行为的表现,目的是通过对关键基础设施破坏或使其失去功能,从而削弱国防力量或经济安全
互依赖性(Interdependence)	不同基础设施各组成部分或位置间的依赖性,由于互依赖性,一个基础设施上受到的影响会作用于其他基础设施
入侵检测系统 (Intrusion Detection System)	对手工或通过软件专家系统实施的入侵或入侵尝试进行检测的系统。它依据日志或其他的网络可用信息进行操作。通过对安全日志或审计数据分析,可以检测到对计算机或网络的入侵
计算机网络防护联合特别任务中心(JTF-CND)	国防部计算机和系统防御的核心,用来监控事件和可能的威胁,协调并指导国防部行动的制定以阻止或控制发生的破坏并恢复网络的功能
测量基准(Metrics)	对系统性能的公认量化测量标准
任务关键性系统 (Mission Critical)	处理对可运行性和任务有效性至关重要的信息的系统,它所处理的信息的内容和时间性会影响到职能任务以及应急任务的成功,因此,这些信息必须绝对准确并在需要时可用(包括在传统环境下加密的信息,也包括敏感的未加密的信息)
减缓(Mitigation)	针对基础设施警告和(或)事件的事先计划好并协调过的操作者的响应,旨在减少或最小化冲击;支持并补充应急、调查和风险管理响应;促进重建过程
网络(Network)	由一系列互联节点组成的信息系统
自然灾害(Natural Disaster)	能够破坏或是基础设施失去能力的物理作用。自然灾害同由于疏忽而导致的威胁相对
合作联盟(Partnership)	两个或多个实体间的关系,关系中的每一方都有责任为共同的目标做出一定,但不相等的努力。在这个关系中,公共部门和私营部门均努力保护并确保关键基础设施的持续运行
补丁(Patch)	一种快速修正错误的程序,有时这种修正是暂时的,直到问题能得到彻底的解决
物理安全 (Physical Security)	为了约束和限制非授权入侵而采取的一种措施,用于减少威胁方成功利用关键基础设施脆弱性而成功攻击的可能性,尤其是对付那些直接的物理攻击,如使用常规或非正规武器发动的攻击等
公众信心 (Public Confidence)	公众的信任,建立在如下基础之上:政府保障国防和经济安全以及政府行动符合社会利益的能力;关键基础设施提供期望的产品和服务并符合用户的最优利益的能力
公钥基础设施 (PKI)	为了发布、维持、注销公共密钥证书而建立的框架,包括软件的使用,它融合了很多安全技术
操作建议 (Recommended Practices)	被广泛接受的原则、步骤方法,可以确保通用性、效率和互操作性
重建(Reconstitution)	所有者/使用者指导下的关键资产和(或)基础设施的恢复
红队(Red Team)	由跨学科的模拟敌手组成的一种独立而集中的基于威胁的测试活动,用来发现脆弱性,从而改善信息系统的安全性
可靠性(Reliability)	计算机、信息或电信系统运行时与其设计规范和高度一致的能力

续表

矫正 (Remediation)	用以提高关键资产和(或)基础设施的可靠性、可用性、生存力等性能的预防措施,如各种应急计划、强化的意识培养、训练和教育;商业活动或操作步骤的改变,资产加固或设计过程的改善,系统级的改变(如物理多样性、伪装、冗余性以及备份)
响应 (Response)	针对事件源或事件起因的第三方(不是所有者,也不是操作者)的应急(如医疗、消防、危险或爆炸物处理)、执法、调查、防御或风险管理服务
风险 (Risk)	一个特定的关键基础设施的脆弱性被威胁方所利用的可能性
风险评估 (Risk Assessment)	对威胁和脆弱性评估后的综合结果。风险评估将分析威胁方利用关键基础设施脆弱性所造成破坏或使其失能的可能性
风险管理 (Risk Management)	理解风险、做出决定并执行决定,从而把风险减少到一个可接受级别的过程。风险管理将确定、衡量并把风险控制在一个已定义好的值上
伸缩性 (Scaling)	在尺寸和配置上很容易改变以适应变化情况的能力
部门 (Sector)	(1) 私营和公共经济之一; (2) 工业或基础设施集团,集团中的成员在社会中履行相似的功能(如公众服务等)
部门协调员 (Sector Coordinator)	大多数关键基础设施被私营部门实体拥有并负责运营,每一基础设施部门都将指派一个人来与对应的联邦领导部门的联络官来合作,共同解决同基础设施保护有关的问题,并为这篇国家计划提出建议
部门联络官 (Sector Liaison)	由每1个联邦领导机构指定的、拥有助理部长或更高官衔的人,它将同私营部门的代表合作,解决关键基础设施保护的有关问题,并为这篇国家计划提出建议
嗅探器 (Sniffers)	一种软件或硬件工具,可以在网上监控数据包,以确定它们是否正常到达或工作是否正常
技术 (Technology)	定义广泛,包括过程、系统、模型和仿真、软件以及硬件
威胁 (Threat)	国内外拥有利用基础设施脆弱性发动攻击的能力并怀有破坏国防或经济安全的恶意企图实体。威胁可以是个人、组织或国家
运输 (Transportation)	以物理分配系统为特征的关键基础设施,对支持国家安全和经济利益非常关键。包括国家空间系统、航空线路和航空器、机场;公路、高速公路、汽车个人交通工具;港口和航道以及船只;大宗货运,包括铁路和汽车;输油管,包括天然气、石油和其他危险品运输方式;货运和长途客运;快递服务等
陷门 (Trap Door)	攻击系统的一种方式。通过硬件或软件机制,系统的设计者有意将其藏下,通常的目的是向服务专家或维护程序员提供进入系统的通路
特洛伊木马 (Trojan House)	含有隐藏代码的程序,往往导致非授权的信息获取、复制或破坏
脆弱性 (Vulnerability)	关键基础设施设计、执行或操作特征,它使得关键基础设施易于受到各种威胁的破坏或容易失去作用
脆弱性评估 (Vulnerability Assessment)	系统地检查关键基础设施、基础设施所依赖的互联系统及其信息或产品,以检查安全措施是否充分,确定安全缺陷,评估可选安全措施,验证这些安全措施在执行后的效果
供水系统 (Water Supply System)	以下列内容为特征的关键基础设施:水资源;水库及存储设备;高架渠及其他传输系统;过滤、清洁和处理系统;输水管道、冷却系统及其他供给机制。它保障了居民和工业应用,包括缓解用水枯竭、进行废水处理以及消防等

缩略语见本书最末附录 II。

请求评论

这篇国家计划的目的是用来保护美国的关键基础设施。在来自各方——联邦国防和民事机构、私营工业、各州及地方政府代表的合作下，该篇计划得以问世。

但是，如果缺乏民众（我们的关键基础设施一旦遭到破坏，他们将是受害者）的参与，本文将不过是一堆稿纸而已。因此，我们请您对这篇国家计划提出评论和建议。

请随时联系我们：

CIAO  
1800 G Street, NW  
8<sup>th</sup> Floor  
Washington DC 20006  
(202) 589-3200  
(202) 589-3246 传真

或访问我们的网站：

<http://www.ciao.ncr.gov>

---

### 三、第 13231 号行政令：信息时代的关键基础设施保护

美国白宫  
2001 年 10 月

---



作为总统，利用美国宪法和法律赋予我的权力，为了在信息时代保护关键基础设施的信息系统，包括应急通信以及支撑这些系统的物理资产，现命令如下。

## 1. 政策

(a) 信息技术革命改变了商业交易、政府运转和巩固国防的方式。这三项职能如今依靠一个互依赖的关键信息基础设施网络。本令所要求开展的（关键基础设施）保护工作应当包含很多旨在保护关键基础设施的信息系统的持续不懈的努力，包括保护应急通信以及支撑这些系统的物理资产。保护这些信息系统，对电信、能源、金融服务、制造业、水、交通、医疗健康和应急服务部门而言至关重要。

(b) 美国的政策是防范关键基础设施的信息系统停止运转，以保护人民、经济、关键性的民生和政务服务以及美国的国家安全，并确保任何停运的发生都是小概率的、持续时间最少的、可控的，且造成的损失尽可能小。这一政策的实施应包括自愿的公私合作机制，其中涉及企业 and 非政府组织的参与。

## 2. 范围

为实现这一政策，应当有一个高层次的行政部门委员会负责协调联邦政府开展的各项与信息系统保护有关的工作，且对这些工作具有话语权，并参与到：

(a) 与私营部门的关键基础设施，以及州和地方政府的关键基础设施进行合作并参与其保护，支持企业和学术机构开展的这类工作；

(b) 保护联邦政府各部、局的关键基础设施保护；

(c) 有关国家安全活动。

## 3. 设立机构

我在此设立“总统的关键基础设施保护委员会”（以下简称“委员会”）。

## 4. 进一步授权

本令不改变现有美国美国政府各部、局的授权和角色。《美国法典》第 44 编第 35 章赋予的授权以及其他可适用的法律，规定了高级官员负责联邦政府信息系统的安全。

(a) 行政部门信息系统安全。管理和预算办公室（OMB）主任负责制定并监督政府范围内各部、局使用的信息系统的安全政策、原则、标准和指南的实施，本令第 4 小节（b）所列系统除外。在本节所述范围内，当 OMB 主任发现某行政部、局的安全措施有严重不足时，应当向总统和有关部、局负责人提供建议。委员会应当协助和支持 OMB 主任的此项工作，并对各部、局的信息系统安全保持合理的关注。

(b) 国家安全信息系统。国防部长和中央情报局局长（DCI）应当有责任监督、制定相关

政策、原则、标准和指南，并确保其各自控制范围内其职能所依赖的信息系统的安全。经与总统国家安全事务助理和有关部门、局咨商，国防部长和中情局长应为国家安全信息系统制定安全政策、原则、标准和指南，这些信息系统支撑着其他行政部、局中的国家安全信息的业务运转。

(i) 本小节所要求制定的政策、原则、标准和指南需要提出比本令第4(a)小节更严格的保护要求。

(ii) 在本节所述范围内，当发现某部、局的安全措施有严重不足时，总统国家安全事务助理应向总统和有关部门、局负责人提出建议。委员会，或其常设委员会、特设委员会，应当保持对国家安全系统的安全及系统连续性相关工作的合理关注。

(c) 其他的职责：各行政部、局的负责人。各行政部、局的负责人要对其控制范围内的信息系统进行保护，并将安全维持在足够的水平。这些部、局的负责人应当在合理的拨款范围内对信息安全工作进行投入，以充分满足上述使命。性价比合理的安全应当成为政府信息系统的不可分割的内在部分，尤其是对那些支撑美国国家安全和其他重要的政府职能的系统而言。此外，安全还应当支持，而不是不必要地阻碍各部局的业务运转。

## 5. 委员会职责

与本令第4节所述职责相一致，董事会应当提供政策建议，对关键基础设施信息系统的保护工作进行协调，包括对应急通信以及支撑这些系统的物理资产的保护。在履行这些职责的过程中，委员会应当：

(a) 与私营部门以及州和地方政府的合作。经与有关行政部、局咨商，委员会应当协调与私营部门的合作，并向私营部门进行关于关键基础设施信息系统安全的咨询，含应急通信以及支撑这些系统的物理资产。私营部门包括拥有、运行、开发和提供信息、电信、交通、能源、水、医疗保健、金融服务的企业。委员会还要协调与州和地方政府，以及业界社区和学术界代表、其他相关社会的合作。

(i) 如有提出需求，委员会可以协助制定自愿性的标准及最佳实践，具体方式要符合《美国法典》第15编第7章的要求。

(ii) 与可能受影响的业界协商，包括法律界、审计界、金融界、保险界等，在法律许可的最大范围内，确定双方共同关注的领域。

(iii) 协调高级联络官的活动，这些高级联络官由司法部长、能源部长、商务部长、交通部长、财政部长、健康和公众服务部长、联邦应急管理局主任所任命，对口这些部、局各自业务领域的私营关键基础设施的保护。在开展此项以及其他有关工作时，委员会还应与关键基础设施保障办公室（CIAO）、商务部下属的国家标准与技术研究院（NIST）、国家基础设施保护中心（NIPC）、国家通信系统委员会（NCS）进行协调。

(b) 信息共享。与工业界、州和地方政府以及非政府组织进行合作，确保建立和维护其信息共享系统，以便在政府的网络运行中心、工业界自愿建立的信息共享和分析中心（ISAC）以及其他有关网络运行中心之间共享威胁预警信息、分析结果以及系统恢复所需的信息。在开展此项以及其他有关工作时，委员会应当与国家安全系统委员会（NCS）、联邦计算机应急响应中心、国家基础设施保护中心（NIPC）以及其他有关部、局进行协调。

(c) 事件协调和危机响应。对危及关键基础设施信息系统安全的事件的响应工作进行协调，

包括影响应急通信和支撑这些系统的物理资产的事件。在开展此项工作时，司法部应当通过国家基础设施保护中心（NIPC）、国家通信系统（NCS）负责人以及其他相关部、局，与委员会协调。

（d）行政部门安全专家的招募、留任和培训。经与各部、局咨商，委员会应对有关工作进行协调，确保政府中负责保护关键基础设施的信息系统，包括应急通信和支撑这些系统的物理资产的雇员得到充分的培训和评估。在开展此项工作时，人事管理办公室应当与委员会协调。

（e）研发。针对联邦政府中开展的以保护关键基础设施信息安全为目的的研发工作，委员会应与科技政策办公室（OSTP）主任协调，确保政府在这一领域的工作能够与企业、大学、联邦政府资助的研发中心、国家实验室的工作保持协同。在开展此项工作时，委员会应当与美国国家科学基金会、国防部高级研究计划局和与其他部、局进行协调。

（f）与国家安全机关的执法协调。推进打击网络犯罪工作，协助联邦执法机构获得各行政部、局的必要配合。支持联邦执法机构对涉及关键基础设施信息系统的非法活动进行调查，包括涉及应急通信以及支撑这些系统的物理资产的网络犯罪。还要支持这些部、局与保卫国家安全的机构进行协调。在开展此项工作时，委员会应当通过国家关键基础设施保护中心（NIPC）与司法部进行协调，通过特勤处与财政部进行协调，以及必要时与其他有关部、局进行协调。

（g）国际信息基础设施的保护。支持国务院对国际信息基础设施安全保护国际合作相关问题的协调。

（h）立法。与 OMB 的 A-19 号通知相一致，就关键基础设施信息安全保护的法律问题，向各部、局以及 OMB 主任、总统法律事务助理提出建议。

（i）与国土安全办公室的协调。2001 年 10 月 8 日的第 13228 号行政令赋予了国土安全办公室对关键基础设施信息系统进行安全保护及恢复的职能，这些职能由委员会履行。经与总统国家安全事务助理协调，总统国土安全助理应负责定义委员会在协调物理资产保护方面的职责。

## 6. 成员

（a）委员会成员应来自下述各行政部、局和办公室。此外，感兴趣的联邦部、局可以参加委员会下面的合适的子委员会。委员会由主席和副主席领导，主席和副主席由总统任命。委员会其他成员是下述高级官员或其代表：

- （i）国务卿；
- （ii）财政部长；
- （iii）国防部长；
- （iv）司法部长；
- （v）商务部长；
- （vi）健康和公众服务部长；
- （vii）交通部长；
- （viii）能源部长；
- （ix）中央情报局局长；
- （x）参联主席；
- （xi）联邦应急管理局主任；

- (xii) 总务管理局局长；
- (xiii) 管理和预算办公室主任；
- (xiv) 科技政策办公室主任；
- (xv) 副总统办公室主任；
- (xvi) 国家经济委员会主任；
- (xvii) 总统国家安全事务助理；
- (xvii) 总统国土安全助理；
- (xix) 总统办公室主任；
- (xx) 总统可能指定的其他行政部门官员。

委员会成员或成员的代表必须是联邦政府的全职官员或雇员，或是永久性的兼职官员或雇员。

(b) 此外，作为委员会成员，下述官员应当组成委员会的协调委员会：

- (i) 商务部下属的关键基础设施保障办公室主任；
- (ii) 国家通信系统委员会主任；
- (iii) 首席信息官委员会副主席；
- (iv) 国家安全局信息保障主任；
- (v) 负责业界管理的中情局副局长；
- (vi) 司法部下属国家关键基础设施保护中心主任。

(c) 联邦通信委员会主任可以指派一名代表加入委员会。

## 7. 主席

(a) 主席同时也是总统的网络空间安全特别助理。各部、局应当尽全力，并在法律允许的最大范围内，使主席及时了解到委员会工作范畴内所有信息系统安全工作的情况。经与委员会成员磋商，主席应当发起和主持委员会会议，设定委员会议程。经与委员会成员磋商，主席可以向有关方面提出与国家关键基础设施信息系统安全相关的政策和项目，包括应急通信和支撑这些系统的物理资产的安全。为了确保与国家安全系统委员会（NSC）和国土安全办公室的充分协调，委员会主席应同时向总统国家安全事务助理和总统国土安全助理进行报告。在涉及私营部门的系统及对经济的影响时，主席还应与总统经济政策助理进行协调。在涉及预算事项以及第 4（a）小节所列系统的计算机网络安全时，主席还应与管理与预算办公室主任进行协调。

(b) 主席应在白宫办公厅内有一个合适规模的工作班子。此外，应主席的要求，在法律许可的范围内，各行政部、局可选派其部、局的工作人员进入主席的工作班子，但要经过总统办公室主任的批准。主席工作班子中与国家安全系统、信息战有关的人，还应在总统国家安全事务助理的直接领导下工作。

## 8. 常设委员会

(a) 委员会可以下设常设委员会，必要时成立特设委员会。常设委员会的代表不必来自于委员会成员所在的部、局，还可以包括其他感兴趣的部、局的代表。

(b) 常设委员会和特设委员会的主席应向委员会定期全面报告所开展的工作，以确保各个

常设委员会、特设委员会之间的协调。

(c) 目前已设立如下常设委员会。

(i) 私营部门及州、地方政府合作常设委员会：商务部派出的代表担任主席，与国家经济委员会的代表相协调。

(ii) 行政部门信息系统安全常设委员会：管理和预算办公室（OMB）派出的代表担任主席，这一常设委员会应协助 OMB 履行其由《美国法典》第 44 编第 35 章及其他法律所规定的职责。

(iii) 国家安全系统常设委员会：国防部领导的国家安全电信和信息系统安全委员会（已调整为国家安全系统委员会）作为这一常设委员会。

(iv) 事件响应协调常设委员会：司法部和国防部派出的代表共同担任主席。

(v) 研发常设委员会：OSTP 主任派出的代表担任主席。

(vi) 国家安全和应急通信常设委员会：NCS 的首脑委员会已更名作为国家安全和应急通信常设委员会。常设委员会的报告职能是 1984 年 4 月 3 日的 12472 号行政令的职能外新增的。

(vii) 物理安全常设委员会：国防部和司法部派出的代表共同担任主席，以协调关键基础设施信息系统的物理安全保护工作。这一常设委员会应当与国土安全办公室的相协调，并与数据交流中心的物理安全工作组及信息安全政策协调委员会密切协作。

(viii) 基础设施互依赖常设委员会：交通部和能源部派出的代表共同担任主席，以协调与关键基础设施信息系统互依赖有关的风险评估、威胁评估和脆弱性评估，包括制定有效的建模、仿真及其他分析工具以及开发性价比高的相关工具。

(ix) 国际事务常设委员会：国务院派出的代表担任主席，以支持国务院对美国政府中相关信息基础设施国际问题的协调。

(x) 金融和银行信息基础设施常设委员会：财政部派出的代表担任主席，成员包括来自金融和银行业监管机构的代表。

(xi) 其他的常设委员会：必要时可以成立其他的常设委员会。

(d) 子委员会。每一个常设委员会可以设立必要的子委员会，主席可以决定子委员会的成员。

(e) 提高效率。委员会应当制定工作流程，以更好地履行以前曾赋予政策协调委员会的职责。经与 OSTP 主任的协调，委员会应回顾 12472 号行政令建立的“联合电信资源委员会”的职能，并为其今后的角色提出建议。

## 9. 规划和预算

(a) 委员会应定期制定国家计划。经与国土安全办公室协调，通过对有关的工作需求和资源进行评审后，委员会还应针对关键基础设施信息系统安全，向 OMB 提出对各部、局该部分预算的建议。

(b) 在法律许可的范围内，总统办公室内的主任办公室应当为委员会提供资金、人事及其他管理支持。在法律许可的范围内，各成员单位也应向委员会提供管理支持。国家安全局应确保委员会的信息和通信系统的安全。

(c) 委员会应每年要求国家科学基金会、能源部、交通部、环境保护局、商务部、国防部

以及情报共同体在其各自向 OMB 提交的预算中体现对委员会活动的支持。

## 10. 总统的咨询委员会

委员会主席应当与政府内外的高级专家密切合作，尤其是总统国家安全电信咨询委员会（NSTAC）、国家基础设施咨询委员会（NIAC，本令建立）。上述两个委员会的主席和副主席可以与关键基础设施保护委员会会晤，以提出私营部门的观点。

（a）NSTAC。NSTAC 向总统提供关于国家安全和战备系统的安全及连续性的建议。

（b）NIAC。本令现在建立国家基础设施咨询委员会，向总统提供关于有关经济领域关键基础设施信息系统安全的建议，包括银行和金融、交通、能源、制造业、应急服务等领域。NIAC 成员不超过 30 人，来自私营部门、学术界、州和地方政府，由总统任命。NIAC 的成员应当具有相关的专业知识，一般从工业界中的 CEO（或其他组织中相应级别的人员）中遴选，他们往往负责各自经济领域关键基础设施的信息系统安全，包括银行和金融、交通、能源、制造业、应急服务等领域。成员不能是联邦政府的全职雇员。

（i）总统应当从 NIAC 成员中指定 NIAC 的主席和副主席。

（ii）本令建立的关键基础设施保护委员会应当作为 NIAC 的行政指导单位。

（c）NIAC 的职能。NIAC 应定期开会，以实现：

（i）提升公私部门对关键信息基础设施信息系统保护工作的参与度。

（ii）提出和开发旨在鼓励私营部门开展关键基础设施信息系统安全风险评估的手段。

（iii）监督私营部门信息共享和分析中心（ISAC）的建设，向关键基础设施保护委员会提出如何促进各个 ISAC 与 NIPC 及其他联邦机构合作的建议。

（iv）通过关键信息基础设施保护委员会，向总统提出如何确保与总统经济政策助理进行合适协调的建议。

（v）向负责关键基础设施保护的“领导机关”、部门协调员、NIPC、ISAC 以及关键信息基础设施保护委员会提出建议。

（d）NIAC 的管理。

（i）NIAC 可以举行听证会、开展调查并建立合适的子委员会。

（ii）应主席的要求，在法律允许的最大范围内，行政部、局的负责人应当向 NIAC 提供与关键基础设施信息系统安全有关的信息。

（iii）必要时，联邦政府高级官员可以参加 NIAC 的会议。

（iv）NIAC 成员在委员会内工作没有补贴。然而，差旅费可以解决。

（v）在法律允许的最大范围内，商务部应通过 CIAO 向 NIAC 提供管理服务、人事服务及其他服务，必要时可向 NIAC 提供资金支持。

（e）一般条款。

（i）《联邦咨询委员会法》可适用于 NIAC，除了向国会报告的条款外。

（ii）NIAC 在本令发布 2 年后终止，除非总统在该日期前延续其运行。

（iii）1999 年 7 月 14 日发布的第 13130 号行政令废止。

## 11. 国家通信系统

技术的变化正引发电话、数据中继、互联网通信等技术融合为互联的网络之网络。国家安全系统委员会和国家协调中心应当支持电话、融合的信息、语音网络、下一代网络等在应急通信及国家安全通信职能中的应用。第 12472 号行政令对各部、局的所有授权及赋予的职能都没有改变，除非本令明确指出。

## 12. 反情报

针对国外情报机关的有关恶意活动，委员会的工作应与反情报行政部门进行协调。

## 13. 定密权

根据 1995 年第 12958 号行政令，兹授权委员会主席有绝密信息的定密权。

## 14. 一般条款

(a) 本令没有取代法律规定的任何要求。

(b) 本令没有创设对美国及其各部、局、实体、其官员、雇员或代理以及任何其他人而言所要求的权利或利益，无论是在实体法还是程序法上。

——布什

---

## 四、《保护网络空间的国家战略（草案）》的 53 个重要问题

美国白宫

2002 年 3 月 20 日

---



## 译者注：

2001 年 10 月 16 日，鉴于“9·11”事件以后美国国家信息安全面临的严峻挑战，美国总统布什发布了第 13231 号行政令《信息时代的关键基础设施保护》，宣布成立总统关键基础设施保护委员会 (PCIPB)。委员会成立后的工作之一，便是制定美国的信息安全国家战略。为此，PCIPB 在 2002 年 3 月 20 日委托 SANS 学会发布了《保护网络空间安全的国家战略》的公告，在综合各方专家意见的基础上提出了与国家战略有关的 53 个重要问题。作为其制定国家战略任务的第一阶段工作，PCIPB 希望广泛征求公众的反馈意见，以便于国家战略草案的撰写。

这 53 个问题分为 5 级：家庭用户和小型商业机构、大型机构、国家信息基础设施部门、国家机构和政策、全球。

## 第 1 级：家庭用户和小型商业机构

**1.1 意识 (Awareness)：**为帮助家庭用户和小型商业机构获知并处理其网络空间的安全需求，应该向他们提供何种意识培养项目及援助？

**1.2 援助 (Assistant)：**为了促进家庭用户和小型商业机构更容易地对其系统实施保护，我们需要做哪些工作？Internet 服务提供商 (ISP) 是否应该为家庭用户和小型商业机构履行更多的网络空间安全职能？

**1.3 披露 (Disclosure)：**ISP、软硬件提供商应向家庭用户和小型商业机构发布哪些风险披露？

**1.4 新兴技术 (Emerging Technology)：**哪些新兴技术（如家庭无线网络、家庭与 Internet 的无线连接以及向家庭的宽带连接）给家庭用户和小型商业机构带来了进一步的风险？怎样解决这些风险？

**1.5 宽带活动 (Broadband Initiative)：**如果联邦政府要去促进家庭用户和小型商业机构的宽带连接的更快部署，那么联邦应支持何种程度的安全需求？

## 第 2 级：大型机构

**2.1 责任 (Responsibility)：**企业中的哪些人应该为 IT 安全负责？他们应多久向 CEO 做一次详细汇报？在 IT 安全的监督中，董事会应扮演何种角色？董事会是否需要来自外部的审计？如果需要，审计的频率是多少？由谁审计？

**2.2 最佳实践措施 (Best Practice)：**CEO、董事会和/或审计师应向何处寻求有关的最佳实践措施或标准，以用于 IT 安全自我评估以及 IT 安全策略的制定？

**2.3 披露 (Disclosure)：**企业应该向其股东、债权人、审计师、董事会披露哪些 IT 安全信息？

**2.4 企业级 IT 安全策略 (Enterprise Wide IT Security Policy):** 企业是否应该应董事会或审计师的要求而定期对 IT 安全操作规范做出新的政策声明? 企业是否应该应董事会或审计师的要求而运行某些软件来推行其安全策略?

**2.5 意识 (Awareness):** 企业是否应当要求其雇员参与定期的 IT 安全意识培训? 为开发这些培训项目, 企业应从何处获得援助?

**2.6 内部人员威胁 (Insider Threats):** 怎样才能获得下述平衡: 既能防止内部人员由于不正当使用 IT 系统而对企业造成危害, 又能尊重每个雇员合法的隐私权?

**2.7 合作者和供应链 (Partners and Supply Chain):** 企业同其合作者以及供应链之间的关系会给企业带来什么样的风险? 这些合作关系如何增强或损害了企业的 IT 安全?

**2.8 事件报告 (Event Reporting):** 何种 IT 安全事件应该报告? 向谁报告?

**2.9 威胁和脆弱性信息 (Threat and Vulnerability Information):** 企业怎样才能知道如何去对 IT 安全威胁和脆弱性做出反应? 企业应怎样去判断对威胁和脆弱性做出反应的方式和方法? 企业应如何评估 IT 提供商发布的各种各样的软件“补丁”?

**2.10 IT 提供商 (IT Vendors):** 企业应将其 IT 安全工作外包到何种程度? 怎样去评估 IT 安全提供商? 企业应如何提高其采购的 IT 产品和服务的安全性?

**2.11 风险管理和保险 (Risk Management and Insurance):** 对于企业在 IT 安全方面的花费或 IT 安全的投资回报, 企业该如何去评估其水平? 保险在企业的 IT 安全中扮演着何种角色?

## 第 3 级: 国家信息基础设施部门

### A. 联邦政府

**3.A.1 最佳实践措施和标准 (Best Practices and Standards):** 针对各类联邦政府机构和/或 IT 系统所支持的各种 (机构) 职能来说, 是否应该有一套 IT 安全最佳实践措施、策略, 和/或标准? 应怎样去制定? 详细程度如何? 是否应符合法律法规的要求?

**3.A.2 可追究性、责任以及监督 (Accountability, Responsibility and Oversight):** 应该对联邦政府的 IT 安全执行何种常规审计? 谁负责执行? 应向谁报告? 对结果应采取何种行动? 怎样才能将这些审计与必要的及时矫正行为联系起来?

**3.A.3 拨款 (Funding):** 在很多联邦机构的 IT 安全状况中, 是不是常规的年度预算有时不足以充分地改善其安全状况? 与此相关的拨款活动是否要与联邦政府在修复千年虫问题时所采取的方法相类似? 如果是的话, 该如何去运行?

**3.A.4 跨越各部的活动 (Cross-Department Activity):** 哪些 IT 安全职能应在联邦部级的级别上履行? 哪些应集中履行? 各部局之间怎样才能更好地合作, 以在履行某些涉及 IT 安全的职能时实现规模经济?

**3.A.5 关键职能连入 Internet (Connecting Critical Functions to the Internet):** 网络中的路由器以及其他系统容易受到来自 Internet 的拒绝服务以及其他类型的攻击, 当联邦的某些关键职能通过这些网络履行时, 如何最好地解决由此带来的风险?

**3.A.6 IT 安全人员 (IT Security Personnel):** 联邦政府在合格的 IT 安全人员方面的短缺程度如何? 联邦政府怎样才能改善其对合格 IT 安全人员的招募、教育、在职培训以及留任?

**3.A.7 采购（Procurement）：**采购政策在改善联邦 IT 安全中发挥着什么作用？

**3.A.8 意识（Awareness）：**IT 安全意识培训怎样才能适用于大多数联邦雇员？

**3.A.9 事故报告（Event Reporting）：**联邦政府应怎样更好地满足各部局对其网络和系统上发生的恶意行为的报告的需求？怎样处理这种报告？

**3.A.10 预警、分析、事件响应和恢复（Warning, Analysis, Incident Response and Recovery）：**联邦政府应该拥有哪些系统和能力，以针对 IT 安全事件去发布预警，执行分析并做出响应？

**3.A.11 组织（Organization）：**为了改善联邦 IT 安全，是否需要组织结构进行进一步的改革？如果有必要，应做什么样的改革？

**3.A.12 国家安全（National Security）：**对那些涉及国家安全的联邦机构来说，是否需要进一步的 IT 安全计划、组织结构或功能？

## B. 私营部门

**3.B.1 各私营部门职责（Sectors）：**每类私营部门应承担何种 IT 安全角色？怎样组织这些私营部门级的活动？

**3.B.2 信息共享（Information Sharing）：**信息共享和分析中心（ISCA）的角色是什么？怎样提高它们的工作效果？联邦政府怎样做才能促进与私营部门在脆弱性、威胁、预警信息以及分析活动等方面实现共享？

**3.B.3 最佳实践措施和标准（Best Practices and Standards）：**最佳实践措施和标准在私营部门中扮演何种角色？

**3.B.4 事件响应和恢复（Incident Response and Recovery）：**在事件响应和恢复方面，应该有哪些私营部门级的合作机制？

**3.B.5 数字控制系统（Digital Control Systems）：**数字控制系统以及 SCADA 系统面临着哪些独特的威胁？怎样解决？

**3.B.6 关键职能连入 Internet（Connecting Critical Functions to the Internet）：**某些私营部门的关键职能在其网络与 Internet 以及其他开放的公共交换系统断开连接后，安全性和可靠性是否能得到更大的提高？

**3.B.7 针对某几个特定部门，国家战略中将分别各有一节讨论其具体问题和计划，包括：**

- 银行与金融；
- 能源；
- 运输；
- 电信；
- 信息技术；
- 通用制造业；
- 化学制造业。

## C. 州和地方政府

**3.C.1 组织（Organization）：**州政府是否应成立州级的负责信息共享和事件管理的组织？如果需要，这样的组织应包括州政府内的机构吗？应包括市级以及县级机构吗？应包括州内与关键基础设施有关的私营部门实体吗？州和地方政府是否应参与国家机制中的 IT 安全活动？联邦政府在州和地方政府成立的上述组织中承担何种角色？

**3.C.2 执法和应急服务 (Law Enforcement and Emergency Services):** 除了州和地方政府的其他 IT 安全需求与活动外, 执法和应急服务机构还面临哪些独特的需求以及问题? 如何最好地加以解决?

#### D. 高等教育

**3.D.1 防范来自大学的攻击 (Preventing Attacks from Universities):** 怎样才能既确保学术研究自由, 又能防止大学内的大规模计算能力被攻击者利用, 以免被用来向其他地方发动拒绝服务攻击以及其他的恶意行为?

**3.D.2 防范大学内的攻击 (Preventing Attacks within Universities):** 大学内哪些职能需要高级别的 IT 安全 (如医疗记录、研究试验、发明专利等)? 在大学这样的学术环境中如何才能达到这样的安全级别?

**3.D.3 组织 (Organization):** 大学应怎样去最好地实现相关的组织化, 以解决它们普遍面临的 IT 安全问题? 是否应在国家级别上就大学内的最佳实践措施或标准达成一致?

### 第 4 级: 国家机构和政策

**4.1 培训和教育 (Training and Education):** 面对受过培训的 IT 安全人员的短缺情况, 国家该如何去处理? 受过各级培训的 IT 安全人员的数目要达到多少才合适? 我们怎样才能完成这些培训? H-1B 签证能否部分地解决这个问题?

**4.2 高度安全/可信的计算 (Highly Secure /Trustworthy Computing):** 除了解决当前软件和硬件中的脆弱性问题外, 是否还应将更主要的研究重点放在开发完全新型且更加安全的操作系统软件、计算机硬件以及软硬件的接口上? 应怎样去资助这些研究活动? 怎样鼓励对这类系统的采购?

**4.3 确保 Internet 结构的安全 (Securing the Mechanics of the Internet):** Internet 的通信流控制系统 (DNS 服务器、边界网关协议等) 的安全性能否增强? 能否通过将控制功能从通常的信道中隔离开来, 使路由器变得更安全? 怎样减轻拒绝服务攻击? 在部署更加安全的系统时, 会遇到哪些问题? 怎样解决? 怎样资助这些活动?

**4.4 确保新兴系统的安全 (Securing Emerging Systems):** 在今后 3~5 年内, 哪些信息技术和系统的数量和复杂度将增长? 怎样去预知这些新兴技术的脆弱性? 怎样去避免其脆弱性? 增强性的安全措施怎样才能被无线网络和无线 Internet 连接所广泛吸收? 随着支持 Internet 的无线半自治设备在数量上的增长和功能上的增强, 有哪些安全问题随之而来? 在使用多种无线接入方式与 Internet 相连的 ad hoc 网络中, 会有哪些安全问题?

**4.5 隐私 (Privacy):** 在实现 IT 安全的某些方法中, 会对隐私带来哪些风险? 怎样消除这些风险?

**4.6 互依赖性 (Interdependency):** 我们怎样判断各类关键基础设施之间互依赖的程度? 如何判断某个基础设施中的脆弱性对其他基础设施带来的影响? 在解决互依赖性所带来的脆弱性时, 怎样将解决问题的负担进行分派?

**4.7 法规及市场驱动力 (Regulation and Market Forces):** 联邦和州政府颁布的法规在实现 IT 安全时应担当何种角色? 作为法规的替代手段, 如何通过进一步刺激市场驱动力使其起到提

高 IT 安全的作用？企业的披露政策、内外审计师、董事会、保险公司、责任法、税收政策等分别起着什么样的作用？

**4.8 研究 (Research):** 国家 IT 安全研究的优先级是什么？这些优先级怎样在下列实体间得到实现：企业研究部门、大学、国家实验室、联邦政府资助的研发中心？研究的花销怎样分摊？

**4.9 信息共享 (Information Sharing):** 在联邦政府、州及地方政府、企业、公众之间应进一步实现哪些信息共享？实现这种信息共享的阻碍是什么？怎样才能最好地实现这种共享？有关非授权入侵者以及其他恶意行为的数据怎样才能最好地组织起来并进行分析？哪些系统应负责发布 IT 安全预警？

**4.10 脆弱性修补 (Vulnerability Remediation):** 在标识 IT 安全脆弱性的过程中，个人和企业应承担何种角色？应向谁报告安全脆弱性？用户应以什么方式以及在何时得到通知？为了确保补丁能够被快速使用，提供商或大规模企业用户应怎样发布补丁？关键基础设施运营者以及政府应怎样辨别并除去逻辑炸弹、特洛伊木马以及其他已经隐蔽地安装在系统或网络中的恶意代码？

**4.11 认证 (Certification):** 软件、硬件以及 IT 安全顾问是否应得到认证？如果是，应怎样认证？被谁认证？

**4.12 运营连续性、恢复、重建 (Continuity of Operations, Recovery and Reconstitution):** 在国家级上，为了响应 IT 系统的中断所带来的广泛蔓延的影响，应该有哪些计划、功能以及部署？

**4.13 犯罪 (Crime):** 为了实现政府和关键基础设施的 IT 安全，司法系统应扮演何种角色？当前州/地方政府以及联邦政府的司法系统是否已足够？当前的法律禁令以及刑法是否已有足够的威慑力？

**4.14 国家安全 (National Security):** 如果恶意行为的源头是某个国家，这时我们的政策和行动应该做出哪些变化？

## 第 5 级：全球

**5.1 信息共享 (Information Sharing):** 为了在各国的机构之间实现对脆弱性信息以及恶意行为信息的共享，需要达成哪些协约？

**5.2 合作标准 (Cooperation Standards):** 是否应该有被国际接受的标准，能对上述事项做出说明：哪些恶意行为属于犯罪？这些犯罪该行为应受到何种惩罚？另外，各合作国应当共同开展哪些调查合作？

---

## 五、保护网络空间的国家战略（草案）

美国白宫

2002 年 9 月 18 日

---



## 委员会主席和副主席的信

### 主题：保护网络空间的国家战略

布什总统下令制定这份《网络空间国家保护战略》的目的在于表明美国在其关键基础设施保护问题上的发展规划。这些基础设施和美国公众的生活密切相关。本文是该发展规划的草案。本文的最终形成得益于社会多方的密切合作。这些合作方包括与网络空间的安全状况密切相关的关键性经济实体、州和地方政府、学院和大学以及其他关注网络空间安全状况的组织。

为响应总统号召而成立的关键基础设施保护公共-私营合作联盟的各成员提交了针对各自所依赖的网络空间的保护战略。这些战略的文本已经发布在互联网上。代表其他实体的一些组织最近也已形成，并且开始制定自己的网络空间保护战略。与本主题相关的会议曾在美国境内各处举行，公开发表的 53 个问题也激发了公众参与讨论本主题的热情。事实上，需要做的事情依然很多。由于国家网络资源的绝大多数由政府以外的实体所控制，对于这种合作联盟的成立和讨论进程都是十分必要的。为了确保这个战略现实可行，它必须是一份国家的主体部门都要得到投资并承担责任的计划。

为了进一步吸收并接纳公众对于本战略的各种建议，在未来的几周内，美国境内将继续举办 8 次相关会议。在 2002 年 11 月 28 日前，公众可以通过网站 <http://www.securecyberspace.gov> 提交对于本战略的反馈意见。国家基础设施咨询委员会和主要工业部门、学术界、州和地方政府的领导将依据经由这些会议和该网站得到的建议对这部战略提出他们的评论和咨询建议。总统将在此后的几个月中审阅并批准该战略。

技术将继续快速发展，新的脆弱性和威胁将不断被揭示，当前方案中的某些内容在未来的某天可能失去效力。为了适应这种不断变化的环境，美国的网络空间国家保护战略必须是动态发展的，并且具备持续性。

在可预见的未来，有两件事将会成为事实：美国将依赖于网络空间，联邦政府将寻求一个日益广泛的合作联盟，以制定、实施并改良《保护网络空间的国家战略》。我们邀请您仔细地阅读我们提出的战略并使您的参与和专业技能实现共享。

——主席 理查德·克拉克

——副主席 霍华德·施密特

## 1. 介绍

今年年初发布的《国土安全国家战略》针对的是一种非常特殊且独具挑战性的威胁——美国发生的恐怖主义，并且提出了一个综合性的框架来组织那些主要职能通常与国家安全无关的联邦、州、地方和私营机构的工作。网络空间对于国土安全和国家安全来说都是至关重要的，我们的经济、关键基础设施、国防均要依靠网络空间的安全性和可靠性的支持。因此，《保护网络空间的国家战略》便成为一个执行战略，它同时支持《国土安全国家战略》和《美国国家安全战略》。他描述了用来保护美国的信息系统，使其免遭有意或恶意破坏并不断增强国家抵抗力的一系列活动。本战略与补充性的《国土安全物理保护战略》共同奠定了用来保护国家基础设施的战略性的国家工作的基础。

### 本战略是一个信息之源

本文以及附带的来自私营部门和学术界的在线资料是一种行动战略，美国将采取这些行动步骤来保护其国家经济、国防和关键服务的运行所必需的 IT 网络和系统。那些网络以及使其互联的相关 IT 设备和软件组成了我们的网络空间。

这部国家战略是一个信息之源，我们国家的很多组成部门将在其中描述它们计划采取的行动以及它们用来保护其各自所在的网络空间的安全战略。在这部国家战略中，读者将看到来自美国各类人士的计划以及为这些各类人士提供的计划。他们包括教师、军事官员、隐私专家、医生、证券经纪人、警察、公务员、计算机科学家、州政府官员、公司 CEO、联邦政府官员。

这部战略还是美国人可以获取有关建议的信息之源，不论他们是否是 Internet 家庭用户、小型企业商人、小型企业的首席信息官（CIO）、市长、州长、财富 100 强企业的 CEO，或是一个任意规模的企业董事会的成员。

### 本战略是一个过程

这部国家战略不是写在石头上的。总统关键基础设施保护委员会（PCIPB）准备定期地在线发布新版本的国家战略。在每次更新版本的介绍中，将会强调新版本对旧版本的改动之处。

网络空间中的各受益团体以及使用者们已经制定了各自的子战略。拥有以及操作关键基础设施的各企业的代表们聚在一起，起草了如何使银行与金融、电力、铁路以及其他部门去保护他们各自所在的网络空间的安全。社区学院和很多大学联合起来对如何保护学术机构的网络空间做了规划。大城市的警察和小城镇的治安官们合作探求了执法界的网络空间安全需求。国会

#### 国家战略将在如下情况下得到发展：

- 国家中有更多的部门和团体制定了的网络空间安全战略；
- 各部门和团体的战略随经验而变得更加详细和优化；
- 技术发生了改变，带来了新的安全挑战和新的能力；
- 我们获得了更多的关于如何去改变脆弱性和威胁的知识；
- 先前版本的国家战略中提出的待讨论的观点达成了一致；
- 某些初始的观点变得成熟。



中参众两院的各委员会召开了针对网络安全和相关主题的听证会。数目繁多的国家协会走到了一起，花费数千小时来为这部国家战略添砖加瓦。

这些集团已经制定了很多战略，以期帮助它们去保护由其拥有或操作着的那部分网络空间，因为每个网络空间的用戶都必须扮演其保护网络空间的角色。这一事实不能够使联邦政府逃避其自己的网络空间保护责任，联邦政府的这些责任不在少数，而且已经在国家战略中进行了概括。然而，上面的事实的确突出了这样一个实情：联邦政府是不能仅依靠自己去保护网络空间安全的。我们每个部门和团体，都必须做好自己这部分的网络安全工作。那些努力的积累将使我们获得成功。

为了促使大家讨论，委员会征求了国内各专家的观点，询问哪些关键事项和问题应当在国家

#### 已举行的市政会议

Denver, Colorado	Chicago, Illinois
Portland, Oregon	Atlanta, Georgia

#### 计划将举行的市政会议

San Antonio, Texas	Philadelphia, Pennsylvania
Boston, Massachusetts	Pittsburg, Pennsylvania
New York City, New York	Phoenix, Arizona
San Diego, California	

战略中得到解决。这些积累起来的问题随后被公布在一个由政府机构、协会、私营机构共同赞助的网页上。很多公民提供了他们的观点。现在这部最初版本的国家战略对大多数问题进行了答复，其他问题则归入了“议程框”中，以便于继续在国家范围内讨论。

为了促进在国家范围内对该战略的进一步讨论，总统关键基础设施保护委员会在国家战略发布之前，于 2002 年春天召开了一系

列公开的城市集会。这些集会遍布了国内的很多城市。

此外，隶属于国家商务部的关键基础设施保障办公室和某些州及其地方政府共同赞助召开了一系列的会议，其中包括分别于 2002 年 2 月 12~13 日在 Texas 的 Austin 和 2002 年 4 月 23~24 日在 New Jersey 的 Princeton 举办的国家级会议。

在如上这些活动之外，还将举行很多其他的城市集会和州论坛，维护国家在网络空间安全方面的对话。

国内各处的相关会议及其计划的具体信息将发布在 [www.securecy-berspace.gov](http://www.securecy-berspace.gov)。

#### 总统关键基础设施保护委员会

在进行调查的基础上，布什总统于 2001 年 10 月签发了第 13231 号行政令（信息时代的关键基础设施保护）并宣布成立了总统关键基础设施保护委员会。该委员会是负责美国网络安全的中央执行机构。它由来自 20 多个部门和机构的高级政府官员组成。总统还组建了一系列跨部门委员会，负责向该委员会报告教育、研究、事件响应和互依赖性等问题。

#### 本战略是对其他战略的补充

本战略是对美国的《国土安全国家战略》和《国家安全战略》的补充。其中，“政策与原则”一节和布什总统发布的第 13231 号行政令提供了本届政府对网络空间安全的政策指南。

本战略中的某些章节比其他章节的内容更为具体详尽。但是，作为一个有待发展的国家战

略，它仍然对所有涉及网络安全的主要问题进行了详略适当的讨论。对于联邦政府、国会、州和地方政府、经济部门、高等教育部门和美国的 Internet 消费群体而言，本战略均是一个具有指导意义的行动路线。

本战略在形成过程中接受了包括联邦政府本身在内的很多机构的建议。它并不是对通常的财务和政策决策制定流程的替代。因为本战略中的很多建议并没有描述额外的资源需求，所以在通常的财务和政策决策制定流程中必须对这些需求加以考虑。这些建议中的多数将成为总统关键基础设施保护委员会或其跨机构委员会的工作内容。

本战略的更新版本不仅将反映各部门和机构的相关工作进展情况，而且将反映 2004 财年的财政预算决策以及总统关键基础设施保护委员会或其跨机构委员会的工作内容。

**本战略适用于网络空间**

本战略适用于网络空间。其他适用于网络空间的战略性文件可能源自各种不同的组织和某些有用的材料。考虑到文件大小问题，本战略的打印文本不包括全部参考文献。但是，联机文件提供了这些参考文献的链接地址。打印文本包含如下主要内容：

- 行动实例：网络空间的威胁和脆弱性；
- 指导本战略的政策和原则；
- 本战略的重点；
- 国家战略的 5 级内容（分别适用于家庭用户、大型机构、关键部门、国家、全球）。

本文在各级内容的最后，简要列出了“建议、行动与讨论”。其中，“讨论”部分中的内容最终可能形成某种“建议”，也可能一无所获。“建议”部分的内容将不断得以完善，并在某些情况下可能被独立机构或私营组织采纳，或者成为政府工作计划的一部分。网络空间发生变化可能导致某些建议无法成为现实可行或者性价比合理的项目。在做进一步考虑时必须放弃这些建议。本战略的更新版将及时考虑这些情况。

内容框架样式如下：

级 别		
R1	建议	政府与非政府部门可采用的用于增进网络安全的具体行动
P1	行动	现有的网络安全工作
D1	讨论	需要进一步分析、争议和讨论的重点问题

非政府组织、贸易联盟、学术团体、州和地方政府、公司等机构的站点均提供了对本文的链接。这些站点上的相关内容仅代表该机构的观点，与联邦政府无关。提供这些链接的原意在于国家战略的形成不仅依赖于联邦政府行为，而且需要多方的参与。

我们竭诚欢迎社会各界积极参与本战略的讨论过程，以便加强美国的网络安全，使国家能够在教育、保健、经济、电子政府和国防领域充分享受信息技术的不断革新所带来的益处。只有在加强网络空间安全的基础上，才能够更大程度地造福于我们的国家和人民。

## 2. 网络空间威胁与脆弱性：行动案例

在“9·11”恐怖事件发生后的一周，另一起攻击事件再次使位于世贸大厦几个街区的世界领先级金融服务公司遭受了打击。这起攻击事件对于经济活动打击的危害远大于它所造成的物理危害。问题的严重性不在于它所导致的可估量的巨大损失，而是它为人们可能面对的未来世界蒙上了巨大的阴影。这次名为“NIMDA”（即“ADMIN”的倒序拼写）的攻击对于一个已经依赖于计算机网络的美国而言，不啻为一次警钟。

NIMDA 是一次结合了计算机蠕虫和计算机病毒的自动化网络攻击。它在美国境内迅速传播，并且能够通过不同的途径入侵计算机系统并破坏系统中的文件。它在 1 小时内便传遍美国，并在短短几天内便感染了多达 86 000 台计算机。NIMDA 给受到良好保护的企业造成了严重危害，迫使公司断开网络连接，关闭客户访问，甚至导致某些公司不得已重建整个系统。由于缺少追踪由此而造成的损失持续性方法，我们无法确定 NIMDA 造成的确切经济损失。但是，据业界资料显示和估计，通过恶意代码实施的攻击行为在 2001 年造成的经济损失高达 130 亿美元。

在 NIMDA 爆发前的两个月，一种名为“红色代码”的网络攻击在 14 小时内便使 150 000 台计算机系统遭受感染，造成了数十亿美元的经济损失。这些事件证明了网络攻击具有日益增加的复杂性和破坏性。同时，攻击的次数也迅速增加。CERT 的统计数据表明，1998 年有 3 700 起攻击事件发生，2002 年则增加超过了 110 000 起。其他机构的统计资料同样表明网络攻击的动态增长趋势。这一趋势仍将继续下去。

### 当今的美国与网络空间息息相关

在美国，信息技术的革新已经悄无声息地改变了经济活动和政府职责的运行方式。在没有对安全问题进行充分考虑的情况下，国家便将对于制造业、设备业、银行业、通信业的关键程序的控制权交付给了联网的计算机。交易的成本也因此而得以下降，产量也得以大幅度提高。更大范围地应用网络系统势在必行。

2002 年，美国的经济和国家安全已经完全依赖于信息技术和信息基础设施。彼此相联的网络支持着所有经济部门的运行。这些部门包括：能源（电力、石油和天然气）、运输（火车运输、航空运输和海洋运

#### 行动案例——主旨

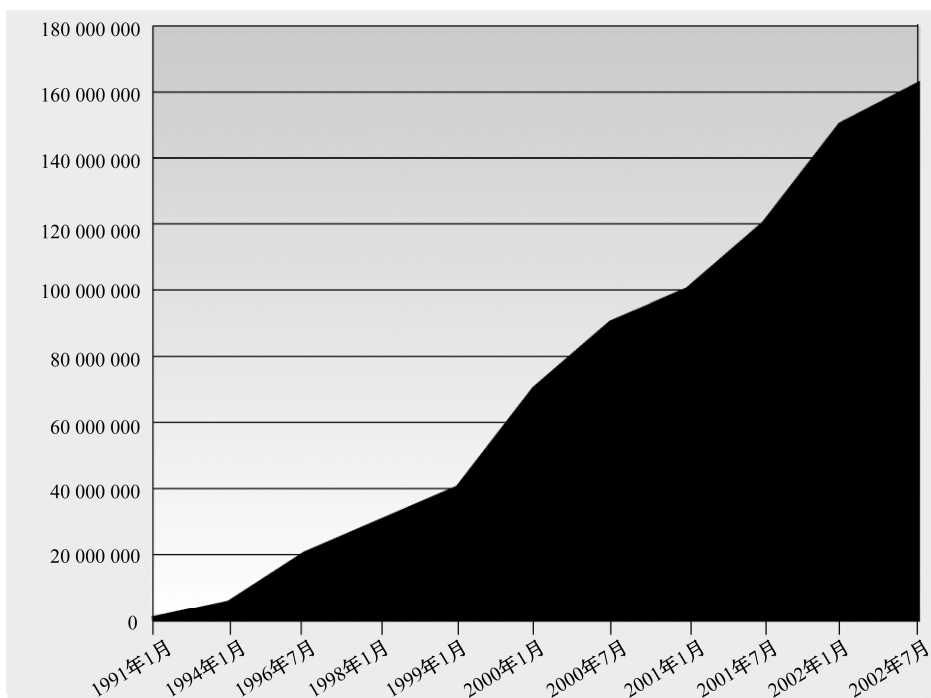
- 网络空间安全事件发生的次数、事件的复杂程度、事件的严重性和代价正在增加。
- 国家经济对网络空间的依赖程度在增加，这导致了尚不可知的依赖关系和单点失败的可能性。
- 一些企业每天都面临着数字灾难。基础设施的受损对这些企业的网络与物理安全状况具有巨大的影响。
- 在威胁发生之前修补脆弱性将削减安全风险。
- 认为过去发生的网络空间破坏行为将对未来可能发生的破坏事件具有指导意义是错误的。事实是将发生的事件可能更为糟糕。
- 通常意义下的网络空间防护依赖于公共-私营部门间的合作。
- 所有人都必须积极行动起来，实现其各自所处网络空间的安全性。

输)、银行与金融、信息与通信、公众健康、应急服务、供水、化学、国防工业基地、食品、农业、邮政和船运。对这些计算机网络的应用进一步扩大了网络空间。这些计算机网络同时也控制着电子传输、火车、输油管道、化学容器、雷达和股市等物理载体。

**Internet** 是我们所依赖的信息基础设施的核心。设计它的初衷是使科学家能够共享无密级的研究成果,并且假设这些科学家不会将该网络用于其他目的。与最初的 **Internet** 类似的网络如今已经连接了数百万的计算机网络。美国的关键服务正是依赖于这些网络得以正常运行。在 **Internet** 迅速发展的过程中,它的安全问题也日益突出。世界各地的人们都可以通过与 **Internet** 相联的网络访问到位于美国境内并支持关键功能运行的网络。

攻击美国信息网络的行为时有发生。所造成的后果包括:破坏关键功能的运行,导致财政和知识产权的损失,甚至危害公众的生命。为了降低现有网络的脆弱性并确定和阻止可能危害美国国家基础设施的网络攻击,必须使网络具有目前所缺少的强健性。

对受害主机数目的调查如下图所示:



### 威胁的范围

针对美国国家信息基础设施的攻击者有很多种,具体包括:从 **Internet** 上下载恶意软件并在网络上随意扰人的攻击者;仅仅试图证明其卓越破坏技术的黑客;利用其访问权限进入计算机系统并造成破坏的受信任的内部人员;在网络上专门实施欺诈、威胁、盗窃的犯罪性组织;正在对美国进行间谍活动并试图发展自己,以便在未来的冲突中破坏美国的经济、削弱或控制美国对其实施反击所依赖的物理资源或网络系统的恐怖分子和敌对国家。

确定事实上的或可能的攻击者有两层目的:不仅应阻止其实施攻击行为并将其绳之以法(例如,传统意义上对于犯罪分子的惩治,网络战意义上的军事行动),而且要通过掌握其攻击技术进一步增强对于国家网络空间的保护。

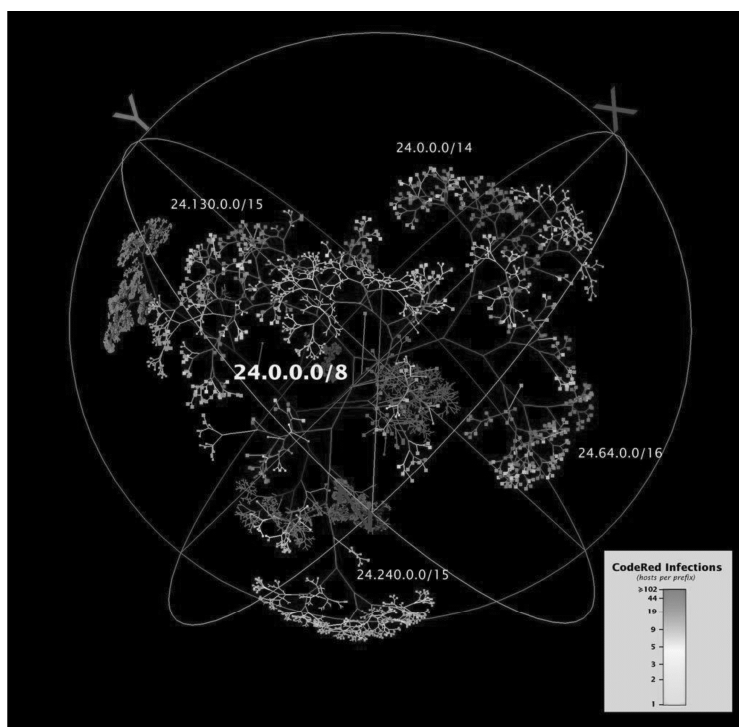
### 在未知的威胁面前减少网络的脆弱性

虽然美国必须应对具体的威胁，但直至获知某个被确定的攻击者的攻击行为后方才修补基础设施中的严重脆弱性是一个具有极端风险的战略，这无法抵御潜在的威胁。2001 年爆发的“红色代码”和 NIMDA 便在任何预警的情况下迅速席卷了美国全境，很多受害者甚至没有机会在遭受攻击之前得到报警信息。即使他们得到了报警信息，很多人也缺少必要的时间、知识和工具保护自己。实施相应的防护措施在某些情况下需要投入若干天时间。

由此得到的教训是：任何依赖于联网的计算机系统的人们必须及时确定并修补系统的脆弱性，而非被动地阻止已经发生的攻击行为或收到报警信息。虽然目前仍然没有捕获制造“红色代码”和 NIMDA 事件的元凶，但必须强调的是：计算机攻击属于严重犯罪行为之列，攻击者被成功捕获的概率正在逐渐上升。

通过信息安全技术审计专业小组来确定系统脆弱性通常需要 2~3 月。通过建立多层防护和韧性网络来修补系统中的严重脆弱性将需要更多月。必须有规律地定期重复这种修补系统脆弱性的过程。

“红色代码”在全球的传播示意图如下图所示：



### 新的脆弱性需要持续的响应

因新的脆弱性会不断形成或被发现，必须持续性地实现网络与系统的安全性。CERT/CC 指出，网络事件和攻击行为发生的次数正在迅速增长并且引起了广泛关注，攻击者可利用的脆弱性亦是如此。已确定的计算机安全的脆弱性（即允许非授权访问或破坏网络的软件与硬件问题）数量在去年迅速增加，由 2000 年的 1 090 起上升到 2001 年的 2 437 起。

安装网络安全设备并不能代替对于网络安全防护状况的持续更新和关注。计算机安全学会

近期的一项调查表明：虽然 90% 的系统安装有防病毒软件，但这些系统中依然有 85% 感染了计算机病毒；虽然 89% 的系统安装有防火墙，60% 的系统安装有入侵检测系统，但这些系统中依然有 90% 有安全漏洞，40% 遭受了外来的入侵。安全实施能够削弱大多数安全脆弱性。这些调查数据表明，好的安全实施并不仅仅是安装安全设备，还包括正确地运行这些设备以及对其定期地打补丁和更新病毒库。

### 网络空间安全及其机会成本

对私企或者国家经济整体而言，增进计算机安全状况都必须投入精力、时间和资金。布什总统已经要求国会在 2003 财年的支出中将用于实现联邦计算机安全的资金增加 64%。

通过节约成本的电子政府解决方案、现代化的企业管理模式以及减少浪费和欺诈的途径，布什总统在联邦计算机网络安全方面的投资将最终减少花销。

缺乏可信、可靠和安全的信息系统已经阻碍了国家经济，尤其是信息技术工业的进一步发展。信息技术的革新对于经济持续增长的促进作用也因此而受到制约。包括电子商务和 B2B 模式在内的发展契机也受到了计算机安全风险的制约。网络空间的脆弱性不仅给这些交易活动带来了很大风险，也威胁到了知识产权、商务运行、基础设施服务和客户信任。

调查表明，对于网络安全的资金投入将带来回报。

- 一次严重的计算机攻击导致的资金投入很可能大于网络安全计划的前期投入。
- 在企业信息系统体系结构中采用强安全策略能够减少整体运行成本，具体途径是采用能够节约成本的安全过程，例如，在缺乏适度安全性的网络中禁止实施远程访问以及客户或供应链的互动。

这些结果表明，通过提高对于这些问题的意识，公司能够通过改善其网络安全状况而受益。更清晰的意识和自愿性的努力是本战略的关键所在。

### 个人与国家的风险管理

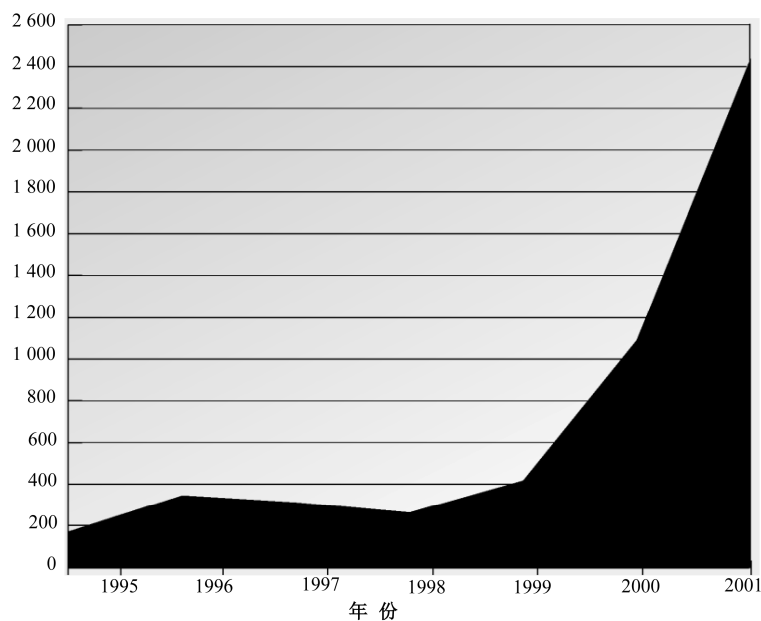
“9·11”事件发生之前，美国境外的恐怖活动对于美国国土造成的危害非常有限。但仅在一天之内，这个情况就被彻底改写了。有人估计，在 4 年时间里通过攻击美国的信息系统而进一步打击美国的经济，前后所造成的损失将是 1:4 的关系。这个相对保守的估计如今也被彻底推翻了。

在美国，每天都有公司或个人家庭用户因网络攻击行为而遭受重大甚至毁灭性损失的事件发生。国家也面临同样的威胁。对于国家所依赖的那些网络和系统：

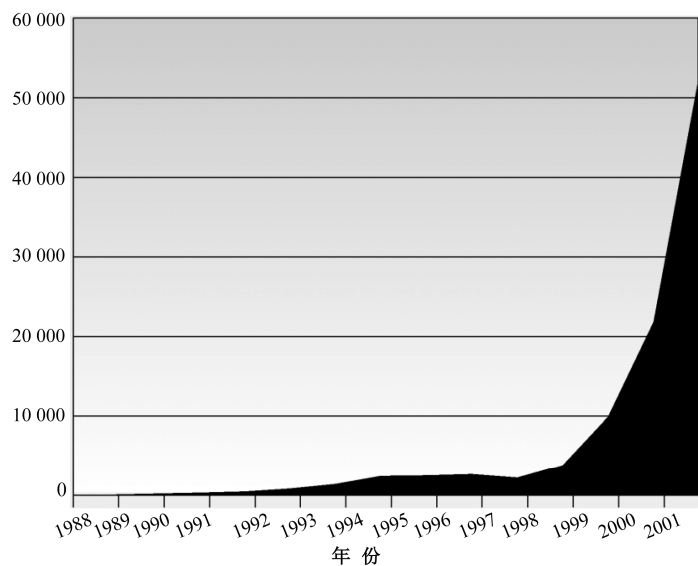
- 潜在对手有实施网络攻击的意图；
- 破坏工具随处可得；
- 国家网络系统的脆弱性众多并且被人熟知。

这些因素表明，没有一个战略能够彻底消除所有风险。但是美国能够而且必须采取行动，尽职尽责地对这些风险进行管理，将通过利用脆弱性所造成的危害降至最低程度。本文作为一份公开文件，不包括潜在对手尚未知晓的具体内容。1997 年，总统委员会曾在一份公共报告中讨论过某些风险；2000 年，发布了第一部有关的国家计划。2001 年，布什总统通过签发行令，将网络空间安全问题列为最重要问题之一，并增加了用于增强联邦网络安全的资金投入。2002 年，布什总统进一步组织并强化了联邦网络空间安全机构。

CERT-CC 报告的脆弱性数目（1995—2001 年）如下图所示：



CERT-CC 报告的事件数目（1988—2001 年）如下图所示：



### 政府单独行动无法实现网络空间的安全

尽管有足够的意识并采取了很多措施，安全风险依然威胁着美国的信息网络和关键系统。降低这些风险要求美国和其全球合作方的各个组成部分共同构建一个主动且前所未有的合作关系。

联邦政府不应该，同时也无法实现私营银行、能源公司、运输公司或其他私营部门的计算机网络的安全。联邦政府不应为实现家庭、大学、地方政府和部门的计算机网络安全化而侵犯

他们各自的活动。

所有依赖网络空间和信息网络的美国公众必须对其所拥有或负责的信息网络的安全状况负责。

联邦政府将通过以下途径帮助美国公众：

- 增强意识；
- 分享关于脆弱性及其应对方案的信息；
- 增进私营组织以及其他团体之间的合作；
- 促进技术的发展；
- 培训专业人员；
- 调查和惩治网络犯罪行为；
- 保护联邦计算机；
- 增强国家经济和安全所依赖的网络的安全性。

归根结底，网络不应该是一个弱肉强食的场所。它是一个采取防范措施便会有所回报的场所，体现着资金投入的效果，关系着美国的安全与否。美国的物理基础设施自 19 世纪建成以来便受到了良好的保护。例如，通过铁路警察的监督降低了大规模运输网络面临的威胁。如今物理安全问题依然存在，但是已经被网络空间的安全问题所超越，这两个问题是相关联的。网络安全能够影响物理基础设施的安全，反之亦然。政府和业界必须对这二者之间的相互影响和独立性进行分析，但同时也必须对网络空间中独特且新兴的脆弱性问题给予特殊关注。

### 3. 国家政策与指导原则

《保护网络空间的国家战略》是对美国的《国土安全国家战略》和《美国国家安全战略》的补充。本节内容和布什总统发布的第 13231 号行政令一起提供了政府对网络空间安全的政策指南。本节所阐述的政策说明和建议均遵从第 13231 号行政令和其他相关的行政令，而没有改变依据国家安全法案或其他相关法律条文所设立的政府机构的职权、分工和责任。

本文是美国历史上第一部《保护网络空间的国家战略》。其目的在于部署网络空间保护工作，赋予该工作的权限。使美国投入到这个领域中来是一项极为复杂和艰巨的使命，要求包括联邦政府、州和地方政府、私营部门和美国公众在内的社会各界的广泛参与和大力合作。本战略将用于实施针对网络空间保护的总统国家政策目标与原则。

#### 国家政策说明

信息技术的突飞猛进已经改变了商业运行方式、政府职能运行和国防实施方式。这三项功能如今密切依赖于彼此相互依存的关键信息基础设施网络，即“网络空间”。

对关键基础设施中的信息系统（包括应急通信、支持这些系统运行的物理资产）进行保护并将其受损害程度减至最低、最大程度地提高系统可靠性仍需进一步的努力。

美国将努力获得并保持对国家基础设施进行保护的能力，以使这些设施免受自然事件和具有如下目的的人为事件的破坏：

- 危害由联邦政府执行关键的国土安全和国家安全保护使命，危害联邦政府保护公众健康与安全的能力。
- 危害州和地方政府维持本地秩序并提供必要的公众服务的能力。



➤ 危害私营团体确保经济有序运行并提供必要的基础设施服务的能力。

需要强调的是，不存在完全可靠的安全措施。但是，必须确保针对这些基础设施的危害具有历时短、频率低、可控、地域上可隔离的特点，并且确保这些危害对美国利益的损害程度最低。

美国的很多关键基础设施是物理上和逻辑上彼此独立的系统。但是信息技术的发展和效率提高的必要性已经加速实现了这些系统稳定并且快速增长的自动化性能和彼此间的互联。

美国的 PATRIOT 法对关键基础设施的定义如下：“一旦缺少或遭受破坏便可能对国家安全、国家经济安全、美国公众健康与安全或这些情况的组合情况造成影响的物理形式或虚拟形式的系统或资产”。美国的关键基础设施包括能源（电力、石油和天然气）、运输（火车运输、航空运输和海洋运输）、金融和银行、信息与通信、公众健康、应急服务、供水、化学、政府服务、国防工业基地、食品、农业、邮政和船运。

本战略认为，要在长时期内维持国家经济和社会的完整性，不仅必须关注信息系统的安全性，而且要关注这些系统所依赖的相关社会结构。因此，本战略综合考虑了增强和讨论这些支持性结构的可行措施。

虽然美国是具备最强大的军事实力和经济实力的国家，这二者却日益依赖于包括基于网络空间的信息系统的关键基础设施。“9·11”事件表明，美国的敌人（无论是国家、组织或个人）将可能采用某种并不便捷的方式对美国实施打击。这些敌手已经明确表明了他们的意图：不仅要打击美国民众，而且要摧毁美国经济的支柱——基础设施和网络空间。

### 政策原则指南

2001 年 1 月，联邦政府着手调查了信息系统和网络空间在美国社会中的地位。2001 年 10 月，布什总统签发了由一系列持续性举措为内容所构成的 13231 号行政令，用以实施一项改进关键基础设施信息系统安全状况的保护计划，包括应急通信和支持这些系统的物理资产。对于网络空间的保护与各经济部门密切相关。该计划的实施得到了如下部门原则性的指导。

#### （1）加强私营-公共部门间的合作

由于美国约有 85% 的关键基础设施由私营经济部门拥有并负责运行，而关键性的政府运行又依赖于这些私营团体，关键基础设施保护必须由多方合作才能进行。

由于针对国家关键基础设施的攻击行为的目标可能同时涉及经济部门和政府机构，所以对于系统潜在脆弱性的讨论，必须采用可同时适用于公共和私营团体、保护本国和国际安全利益的灵活、易更新的途径。私营经济部门已经积极参与了与政府机构的密切合作。在此过程中，信息共享和分析中心（ISAC）的建立是一个重要途径。这些中心简化了私营经济部门共享和发布安全相关信息的方式。此外，各经济部门已经制定了保护各自网络空间的计划，这些计划均是对本战略的补充。政府希望并且鼓励此类有效的合作方式。

美国必须集中精力致力于防范机制与危机管理，具体包括：确定并修补网络系统的脆弱性、教育培训、研究与发展、预警方法以及发展相关的支持措施。在此意义上，私营机构必须确保所控制的基础设施具有最大可能的安全性，并向政府提供有关的必要帮助信息。联邦政府在保护己方信息系统安全的同时，必须努力成为各私营部门模仿的典范，向其示范获得基础设施保障的最有效同时也是最可取的途径，并发布互惠互利的实践经验。

#### （2）避免（过于依赖）法规

为了鼓励私营企业，联邦机构指出，私营-公共合作团体中的所有者和运营者必须多样化。为了鼓励私营企业最大程度地参与合作，美国政府尽己所能地避免可能形成政府法规或增加政府对于私营企业约束力的政府行为。因此，政府在关键基础设施保护过程中将主要依赖市场调

节与激励作用，仅在这种途径对于美国民众的健康、安全和福利的保护无效的情况下，才借助于行政权。

(3) 保护公众自由与隐私

安全的利益和个人隐私不应彼此冲突。事实上，通过保护 Internet 上通信的整体安全性，本战略所倡导的各项措施均以保护个人隐私并进而保护个人安全利益为目的。然而，在采取措施来增进国家安全的同时，必须避免对国家尽力维护的这些自由社会中的基本价值观和特征造成破坏。因此，必须保护隐私和公民的其他自由。消费者和实施者必须确信信息处理的方式是正确、保密和可靠的。

(4) 与国会保持协调一致

为了确保以实现美国的网络空间系统安全性为目的而采取的行动得到广泛的支持，行政机构将与国会在具体措施和流程上进行合作，以便使其行动与国家政策的目标保持一致。在适当的情况下，行政机构可以请求国会通过立法促进本战略的实施。

(5) 与州和地方政府进行合作

美国式的民主来源于联邦制——一种由州政府与联邦机构分享治理权的政府组织结构。联邦政府、州政府和地方政府共存的形式导致出现了 87 000 个不同的司法机构，从而为网络空间安全工作提出了独一无二的机会和挑战。与联邦政府一样，州政府和地方政府也拥有并运行着规模庞大并且彼此相联的网络系统，关键性的政府服务也依赖于此。这些网络系统的安全性由本地专家和地方性机构与组织中与网络安全相关部门来负责维护。他们必须对该网络系统进行互联和扩充，以便它们得以巩固而非复杂化，并且满足必要的应用要求。因此，所有的关键基础设施和网络空间保护计划与实践都必须考虑需求、实践性和州政府、地方政府以及第一响应员各自所应承担的责任。

合作机构

为简化并增强联邦机构与有效合作所依赖的私营部门的合作与交流，政府为容易因基础设施遭受攻击而受影响的各主要经济部门指定了“领导机构”。这些机构及其相关机构见下表：

领导机构	部 门
国土安全部	<ul style="list-style-type: none"><li>➢ 信息与通信；</li><li>➢ 交通运输（航空、铁路、大宗货物运输、水路货运、石油与天然气管道运输、高速公路（包括汽运与智能运输系统）；</li><li>➢ 邮政与船运；</li><li>➢ 能源服务；</li><li>➢ 政府持续性</li></ul>
财政部	<ul style="list-style-type: none"><li>➢ 银行与金融</li></ul>
健康和公众服务部	<ul style="list-style-type: none"><li>➢ 公共健康（包括疾病预防、监测、图书馆服务与个人健康服务）；</li><li>➢ 食品（不包括肉类与禽类）</li></ul>
能源部	<ul style="list-style-type: none"><li>➢ 能源（电力、石油与天然气生产与储存）</li></ul>
环境保护局	<ul style="list-style-type: none"><li>➢ 供水；</li><li>➢ 化学工业危险材料</li></ul>
农业部	<ul style="list-style-type: none"><li>➢ 农业；</li><li>➢ 食品（肉类与禽类）</li></ul>
国防部	<ul style="list-style-type: none"><li>➢ 国防工业基地</li></ul>

此外，科学技术政策办公室（OSTP）为支持基础设施保护而负责对研究与开发活动进行组织协调。管理和预算办公室（OMB）负责为联邦政府的计算机安全项目制定政府性政策、原则、标准和指南，并预见其可能的实施后果。国务院负责协调国际性的网络安全事项。中央情报局局长负责评估其他国家针对美国的网络与信息系统的威胁。司法部和联邦调查局负责调查和惩治网络犯罪。

各基础设施部门的代表和联邦领导机构在通力合作的基础上将评估这些部门的脆弱性对于网络空间安全或物理安全的危害，并提出消除严重的脆弱性的计划和措施。由于针对国家关键基础设施的技术和威胁仍将继续迅速变化，基础设施部门和领导机构必须经常性地对关键基础设施的可靠性、脆弱性和所处的威胁环境进行评估，并且采取具备足够灵活性的保护和响应措施。最后，为了维持合作关系，包括执法、行政规则、外国情报、国防力量在内的全部政府法令、职能和可供利用的资源必须全部就绪并且可用，以便尽可能地确保并维持对于关键基础设施的保护。

### 指导性的战略原则

网络空间安全国家战略是遍布美国境内的很多个人、团体和研究机构共同努力的成果。这些努力的最终目标是建立一个在未来可预见的时期内能够支持美国的经济、国家安全和关键性服务的安全、可信、强健、可靠并且可用的基础设施。

网络空间是一个连接了各种基础设施、企业和国家的复杂网络。其中的网络连接涉及由很多不同运营者所拥有的众多网络。实现该网络的安全性不同于确定其某个组成元素或连接路径的是否正常可用，而是必须确定网络整体是否具有对于破坏行为或信息丢失的抵御能力，确定某个网络路径是否可由其他路径替代，确定网络的组成元素是否具有冗余并且永久失效的可能性很小。网络空间中的单个元素的安全性及其在颇具变化性的环境中的不断更新是其具备上述抵御能力的基础。

因此，为建立一个安全并且韧性良好的网络空间，美国必须遵循以下两个战略性的安全原则：①整体基础设施的安全性依赖于其各个组件的安全性；②威胁和脆弱性将不断更新，因此安全性必须具有与之相等或更高的更新速度。

#### （1）分部分保护，最终实现整体安全

网络空间的安全性依赖于其中各个组件的安全性。在网络空间中，发生在某处的攻击行为可能以光速传播至其他各处。地理安全的概念将不复存在。网络不仅对于外部攻击而且对于内部攻击都具有脆弱性。一个安全网络的组件安全性可能由于内部人员、下载的软件或遭受攻击的邻近组件而受到破坏。只在网络的外围设置一堵安全墙是不足以确保网络的安全性的。

一旦网络中的某台计算机或某个组件被破坏，它便能够被用于进一步破坏网络中的其他计算机或组件。与之类似，经济或政府中的非安全部门也能够被用作对其他部门实施攻击的平台（而且这些事件已经发生了）。某个部门遭受破坏也具有扩散效应，从而影响和破坏基础设施中的很多其他组成部分。为了应对这些脆弱性，基础设施的安全绝不应该仅依赖于某个单层、一组节点或主要节点，而是必须体现在多个层次上的分布式防御中，以及体现在遭受任何攻击后均能够迅速恢复的能力中。

为了提高网络空间的安全性，美国必须在行动的各个层次上实现网络空间的安全。个人和单个的部门必须意识到自己在此意义上的角色和应承担的责任。各部门和个人实现网络空间安

全的努力彼此相关。因此，美国必须通过以下途径实现网络空间的安全：意识培养与信息传播；各层次上明确的角色和合作关系；联邦网络系统安全化中的联邦领导能力。这里，联邦领导能力也包括防止和阻止网络犯罪、电子欺诈和信息战。

(2) 为获得技术优势并提前预防系统脆弱性，迅速革新安全措施

系统脆弱性的增加速度非常惊人。新软件的开发和新技术的出现均会带来新的脆弱性。随着时间的推移和这些软件与技术的应用上的推广，这些脆弱性将逐渐被发现。与此同时，用于发现这些脆弱性的新工具或由原有工具演变而来的高级工具也会随之出现。安全政策、实施和技术必须相互适应。美国必须开发一种能够优于攻击者能力发展的安全基础设施。

有关专家目前已开始考虑纳米技术和量子计算对当前的网络空间可能造成的影响。这些（以及其他）新事物将使网络的运行方式和网络安全的实现方式产生无法预知的变化。为了理解这些变化并保持美国在网络空间安全新技术的开发与应用中的世界领先地位，美国必须在教育与培训、技术以及协调活动中进行投资。

## 4. 本部战略的重点

本节将概要描述后续章节的内容并给出框架。

### 战略

网络空间的安全密切依赖于下自家庭用户上至联邦政府的全部国家网络基础设施的所有者。全部的个人与组织均需负责自己所在部分的网络空间的安全性。制定本战略的目的是赋予个人与组织在此意义下所需的能力。本文针对如何获得网络安全提供了发展方向，同时也提供了使所有美国人进一步具备该能力所需的工具。

为建立本战略的蓝图，网络空间的各主要组成部分已经着手致力于制定针对各自基础设施的保护计划。其中某些计划已经取得了进展，并在本文有所描述。有关其他计划的内容将陆续被加入。这些计划将共同体现私营部门、政府和个人在积极建立、维护和更新网络空间安全方面所进行的合作。

整体的国家战略目标是赋予美国公众保护自己所处的网络空间的能力。这一战略目标的实现将采用以下六个用于实现上述能力的工具：

(1) 意识培养与信息传播：对网络空间的用户与系统所有者进行教育，使他们知晓各自系统中的风险与脆弱性以及减缓这些风险可采取的措施。

(2) 技术与工具：开发更为安全的新技术并迅速应用这些技术，以更加安全的方式应用当前已有技术。

(3) 培训与教育：开发一支庞大并且高水平的网络空间安全队伍，以便满足业界与政府的需求，革新并增进国家的安全空间维护能力。

(4) 角色与合作关系：通过利用市场驱动、教育与志愿者活动、公共-私营部门的合作以及法律法规强化处于各个安全级别上的个人、企业与部门的职责。

(5) 联邦的领导：通过以下途径增进联邦的网络空间安全：增加可追究性；实施最佳措施；在持续性的测试、监视与安全实践更新中广泛使用自动化的工具；采购安全且经认证的产品与服务；进行先进的培训并促进技术人员的发展；防范和阻止网络攻击行为的发生。

（6）协作与危机管理：在公共、私营部门内部及其相互之间采取预警并实现信息共享，以便对攻击行为进行快速检测并做出有效响应。

本战略将以如下两种方式反映这些主旨：①在对各部门的介绍中将说明与之相应的战略目标；②在有关该部门的具体内容中重点说明以实现该战略目标为目的正在执行的计划、建议和讨论主题。

本节将概要描述这些战略和支持性内容。这部国家战略将为行动方案提供新的建议，并提出为数众多的新问题和有待进一步争论的主题。联邦政府的目标是以此推进在这些争论的基础上形成建议的过程。某些建议将得到进一步发展；反过来，一些建议甚至将成为个人、组织或政府的行动。

#### （1）各部门的建议概要

本部国家战略号召各级基础设施部门进行响应。以下是本战略号召的一些需要集思广益的主要创新。后文将对这些内容进行深入讨论。

#### （2）意识培养与信息传播

本战略指出：必须提高对于美国的关键基础设施中所存在的脆弱性的认识，必须提供有助于个人、公司、组织和机构参与增进网络空间安全性而所需的信息。这部分建议包括：

- 家庭用户和小型企业应该意识到它们在实现网络空间安全中的重要角色，包括实现其各自计算机系统的安全性、依据众多站点（包括 [www.StaySafeOnline.info](http://www.StaySafeOnline.info)、[www.nipic.gov](http://www.nipic.gov)、[www.crsc.nist.gov](http://www.crsc.nist.gov)）所提供的信息以安全的方式访问 Internet。
- 总统关键基础设施保护委员会下属的意识委员会应加强公共-私营部门的合作，以便开发和传播网络空间安全意识培养材料，尤其是针对不同群体的且可用于年度意识培养的工具与资源。
- 州和地方政府以及私营实体应该针对不同年龄阶段的学生确定并提供包括如下内容的指南：网络空间意识、文化、培训、教育（包括网络空间中的道德行为教育）。

#### （3）技术与工具

本战略指出：必须增加与网络空间安全有关的研究。这部分建议包括：

- 公共-私营部门的合作应首先尽力开发最好的措施和技术，以提高应用于日常设备、生产制造业以及其他网络中的数字控制系统（DCS）和监督控制与数据采集系统（SCADA）的安全性。与此同时，依赖于这些系统的石油运输管道与电力传输网的所有者和运营方应密切关注网络连接中的风险并采取正确措施，如实施全天候的安全认证。其他密切依赖这些系统的工业界也应有相同考虑。能源部近期发布的指南提供了用于改进 SCADA 系统安全性的信息。
- 总统关键基础设施保护委员会应该与科技政策办公室（OSTP）主任就联邦政府研究项目进行合作，研究计划应该包括短期（1~3 年）、中期（3~5 年）和长期（5 年以上）的信息技术安全研究。联邦政府资助的 2004 财年的短期信息技术安全优先研究项目应该由 OSTP 和 R&D 委员会负责确定。这些项目包括：入侵检测；Internet 基础设施安全（包括 BGP、DNS 等协议）；应用安全；拒绝服务；通信安全（包括 SCADA 系统中的加密与认证）；高保障系统和安全系统集成。
- 公共-私营部门的合作应该确定跨部门的网络空间和物理互依赖性。在《国土安全国家战略》中提议的项目的协作下，应制定有关计划来减少相关的脆弱性。这一目标可

以在国家基础设施仿真与分析中心的协助下达到。

#### (4) 培训与教育

本战略指出了对于合格的信息技术人员的需求与美国在培训这些人员方面的能力之间的鸿沟。这部分建议包括：

- 州政府应该在州立大学中建立网络空间警察服务奖学金计划，以此对同意在毕业后为本州工作作为回报的信息技术专业本科生与研究生进行资助。现有的联邦政府网络空间警察服务奖学金计划应该适当地在更多的大学中得以推广，包括补充师资和提供奖学金资助。该计划也应增加在社区学院中补充师资和提供奖学金资助的内容。
- CIO 委员会和相关的联邦机构应该考虑建立一个负责承担联邦网络安全与计算机取证培训计划的“网络空间研究院”。
- 信息技术安全人员、合作团体和其他适合的机构应该共同尝试确立一种可行的国家级资格认证计划。联邦政府将帮助确立该项计划，并在该计划确定之后考虑要求联邦的信息技术安全人员通过该项认证。

#### (5) 角色与合作关系

本战略指出：全体美国人在网络安全的实现过程中都扮演着各自的角色，同时，可以在实现该安全性的过程中采取市场机制激励现有的相关行动。这部分建议包括：

- CEO 应考虑成立企业安全委员会，负责整体考虑本企业的网络空间安全、物理安全和可操作性。
- 州和地方政府应考虑在其部门和机构中建立包括如下内容的信息技术安全计划：意识培养、审计与标准。地方政府应提供该计划所需的帮助、资料和计划范例。
- 以主要 Internet 服务提供商为首的这些提供商（ISP）应考虑采用“良好的产品规则”制度来管理其网络空间。该制度也适用于不同 ISP 之间的合作。
- 联邦政府应该确定并排除那些阻碍公共-私营信息共享的壁垒，并为增进网络安全而鼓励及时的双向数据交换。
- 学院和大学应考虑联合建立：①一个或多个用于应对网络攻击与脆弱性的信息共享和分析中心（ISAC）；②用于赋予主要信息官员对网络安全进行讨论的范例指南；③一种或多种最优化的信息技术安全实践；④用户意识增进计划与材料范例。

#### (6) 联邦领导

本战略强调使联邦网络空间安全成为美国的网络空间安全范例的迫切性。这部分建议包括：

- 以增加更多安全性产品的采购为目的，联邦政府将在 2003 财年第四季度之前完成对国家信息保障联盟（NIAP）的综合考查，以便做到：①确定 NIAP 在现有资金支持力度下将获得的信息保障程度并明确所获安全性能与目标之间的差距；②该计划是否为消除这一差距而确定了发展目标，是否正在试图缩小这一缺陷，该计划的改进、调整或进一步扩充所能达到的合适并且代价合理的信息保障水平。
- 联邦政府部门应继续扩大自动化的企业安全评测和安全政策实施工具的应用程度，并为免受攻击而积极采用威胁管理工具。2003 财年第三季度结束之前，联邦政府将针对是否有必要采取具体行动以便进一步促进这些工具的使用进行决策。
- 2003 财年第二季度结束之前，针对某个选定的政府部门的业务流程，基于安全和应急战备的演习来考查成本有效性。经过这些演习所发现的任何安全弱点均应包含在各

机构的《政府信息安全改革法》（GISRA）的矫正计划中。

- 联邦政府各部局必须在采用无线技术时对安全风险进行充足的考虑。联邦政府应考虑安装能够不间断地检查网络上是否存在非授权的无线连接情况的系统。联邦政府机构应该仔细阅读 NIST 发布的有关无线技术采用的最新报告并考虑 NIST 的建议。以此为基础，联邦政府机构应该在其机构政策与业务流程中慎重考虑附加风险并采取风险消除措施。这些措施包括强加密、生物认证、保护标准与其他的技术性安全考虑、配置管理、入侵检测、安全突发事件处理以及计算机安全教育与意识培训。
- 机构的年度信息技术安全审计应该包括对于与信息技术相关的隐私规则的审查。

#### （7）协作与危机管理

本战略强调了对于综合性的国家分析与预警特性的迫切需求。这部分建议包括：

- ISP、硬件与软件经销商、与信息安全相关的公司、计算机应急响应小组与 ISAC 应该通力合作，考虑建立一个物理或逻辑形式的网络空间运行中心（Cyberspace NOC），以便为支持美国的 Internet 正常和可靠运行而进行信息共享与合作。该中心可能是一个非政府机构并由私营部门负责管理，联邦政府将与该中心进行合作。
- 业界应该在与联邦政府的自愿性合作中完成并规律性地更新网络安全突发危机应急计划，包括 Internet 功能恢复计划。
- 执法和国家安全界应开发一个用于检测针对国家安全的网络攻击（即网络战）的系统，并制定一个即时响应计划。本过程应该允许适当的部门提出各自的要求和待选方案。
- 信息系统网络与网络数据中心的所有者与操作者应该考虑建立针对突发事件的补救性应急计划，以便减少针对这些网络的大规模物理性破坏所造成的损失。联邦政府将在需要的情况下负责对各参与方进行协调并提供技术援助。
- 为鼓励建立用于检测和阻止网络攻击行为的国家和国际监察与预警网络，美国应该与其他国家、非政府机构（如 FIRST）和国际组织（如 ITU）加强合作。这些网络同时将有助于对网络攻击行为进行调查和响应。

#### （8）针对不同级别用户的六种实施工具

本战略提供了一个帮助美国理解其网络空间安全维护使命的行动路线。为使本战略具有更现实的指导意义，我们将它所涉及的对象划分为以下五个级别：

- 第 1 级，家庭用户和小型商业机构；
- 第 2 级，大型机构；
- 第 3 级，包括政府、私营企业和高等教育在内的部门；
- 第 4 级，国家事务和工作；
- 第 5 级，全球事务讨论。

各级别及其子级别分别具有各自的战略目标。这些目标的实现将得到国家所采取的战略行动的支持。

这六种工具将帮助推动各个级别中的相关行动。其中的部分或全部将在各级上得以应用。例如，“意识培养与信息传播”将帮助家庭用户、私营部门的雇员和联邦政府的工作人员实现其所处的网络空间的安全。不同级别具有各自的“角色与合作关系”描述。并非所有的工具都将被用于各个级别，但是它们将共同促进美国在实现国家网络空间安全方面进行的所有努力。

## 5. 第1级：家庭用户和小型商业机构

本级的战略目标是赋予家庭用户和小型商业中的工作人员保护各自的网络空间的能力，且赋予他们避免这些网络空间被他人利用并实施网络攻击的能力。该目标的实现途径如下：

- 加包括孩子和学生在内的家庭用户和小型商业中的工作人员的网络空间安全意识。
- 帮助家庭用户和小型商业中的工作人员使用防病毒软件、软件补丁、防火墙，这可能要通过 ISP 进行。
- 鼓励并帮助家庭用户和小型商业中的工作人员在所有宽带网连接（包括电缆 Modem、DSL、卫星和无线连接）上安装并使用防火墙。
- 通过地方性机构和教育培训，帮助家庭用户和小型商业中的工作人员掌握网络安全资源。

### 问题与挑战

#### （1）规模太小，不至于成为目标？

很多美国人认为，攻击者所攻击的对象是大型的政府部门和大型机构。他们认为网络安全与己无关。

不幸的是，这种想法并不正确。即使是家庭用户和小型商业，也可能遭受严重的网络攻击，并在某些情况下被攻击者利用，继而攻击其他受害者。具体事例见下表：

针对家庭用户和小型商业机构的网络攻击

可能发生的情况	具体说明
硬盘崩溃	计算机病毒对家庭用户与小型商业用户的计算机所造成的最常见危害是毁坏文件、软件和操作系统。危害的结果可能是出现黑屏或导致数额巨大的修复费用。通常情况下更为重要的是，小型商业或家庭用户可能丢失不可替代的数据（如客户记录或个人通讯录）
身份盗用	家用计算机上存储的信息可以为黑客提供足够的信息，使他们能够通过用户的姓名盗用信用卡号或用户身份
信用卡盗用	与使用新的信用卡不同，黑客可能仅利用家庭或小型商业用户存储在硬盘上的信用卡数据在线购买产品，并将其出卖给出于商业目的而搜集电子邮箱地址的网站
秘密文件传输	当某个公司雇员在家工作并通过网络将某些文件传送到公司时，他人便有可能通过入侵该家用计算机并在待传输的文件中隐藏某个秘密文件，从而将该秘密文件传送到公司的网络
敲诈	对于小型商业，黑客可能通过威胁该企业将其客户信息和信用卡号码公布在某个站点上的途径来给该企业造成损失
Zombies（僵尸）	这是一些能够自动搜索与网络相联但是未加保护的系统的程序。搜索的结果是这些系统在系统所有者不知晓的情况下被他人控制并被用于实施某些恶意行为
伪造私人信息	某些病毒可以将私有或秘密文件由硬盘传输到用户邮件地址的清单中

#### （2）我会遭受网络攻击吗？

不幸的是，本战略所描述的各种网络攻击行为普遍存在于当今美国人生活环境中。由于自动实施网络攻击的工具越来越多，攻击一个甚至所有用户已更加容易。例如，“Honeynet 项目”利用附加在 Internet 上的“dummy”系统评价了实际发生的计算机攻击。依据该项目的最新研究成果，Internet 上任意一台计算机每天被扫描（被检测到其已联网、已安装或存在脆弱性）



的次数至少有几十次。一个普通家庭用户安装的“Honeypot”在4天内被攻击了5次。拥有大型系统的家庭用户或小型商业也是网络攻击的目标之一。系统通过 Internet 遭受某种攻击的日平均数是17次。在某些情况下，一台非安全的服务器在接入 Internet 之后的15min内便受到了攻击。

### （3）安全使用 Internet

目前的 Internet 并不安全。安全使用 Internet 只是一个期望通过提高意识、使用安全服务与工具来达到的目标结果。例如，很多家庭用户和小型商业并不使用防火墙保护其计算机。

保持“一直在线”状态的宽带、DSL、无线和卫星服务正日益流行。这些服务具有很高的连接速率和服务效率。但是，由于很多用户对于“一直在线”状态所可能导致的安全问题没有足够的意识，他们其实正带来日益增多的安全隐患。例如，由于这些连接能够即时并且持续传输大量数据，攻击者便能够利用他们对其他用户实施攻击，攻击的结果可能在全国范围内造成严重损失。

通过为 Internet 用户提供完整的产品链，能够明显推动家庭用户和小型商业以安全的方式应用 Internet。ISP、硬件制造商、软件经销商、零售商和安全服务提供商均能够通过对产品和服务的改进而推进这一进程。

## 战略讨论

### （1）获取安全的五个步骤

有很多地方可供家庭用户、家庭中孩童的父母或小型商业中的用户为避免 Internet 上的安全问题而寻求信息帮助。在访问下文所建议的安全站点之前应考虑如下五个步骤。

#### ①使用不易被猜测出的口令

黑客利用 Internet 上随处可见的口令猜测工具可获得用户口令，并访问用户账号和计算机。使用强口令并定期更新口令非常重要。强口令应该满足以下条件：

- 长度至少8位；
- 混合使用大、小写字母；
- 字母和数字的顺序具有随机性（而非将数字列在口令的最后几位）；
- 选用键盘上的一些特殊符号（如#、\$、&、\*等）。
- 家庭用户应该至少每6个月更新一次口令。

#### ②维护一个及时更新的防病毒软件

每周都会有新病毒出现，并且这些新病毒是造成危害的最主要来源。计算机上安全的防病毒软件很快就会过期，但是可以通过与该软件的生产厂商取得联系来更新软件。目前，很多这类软件的生产商会自动发出更新通知，因此用户可以不必要每周访问相应站点。

#### ③安装并及时更新软件补丁

日常使用的很多软件程序（操作系统、Web 浏览器、E-mail 阅读器等）经常被查出具有某些安全漏洞或缺陷。软件公司会对这种情况发出“再通知”，但是该通知与汽车生产厂家的类似通知不同，它并不通过普通邮件发出。一般说来，用户需要通过访问该软件公司的站点来发现问题并寻找解决方法。这些解决方法通常是从 Internet 上下载少量的被称为“补丁”的附加软件。建议运行简单系统的家庭用户和小型商业使用这些软件（在大型系统中，必须在使用这些补丁程序之前对它们进行分析，以便判断它们是否会与系统中的其他程序发生冲突。）

#### ④过滤

父母可能希望能够通过使用某些软件对孩子使用 Internet 的情况进行控制,以便这些孩子仅能够访问与其年龄相符的站点,并获得适合其年龄特点的网络资料。很多 ISP 提供了这类软件或过滤器,也可以通过私营商获得这类软件。除了对不适当的站点进行过滤外,父母可能还希望限制孩子的电子邮件来源。绝大多数 ISP 允许用户针对自己所有的电子邮件账户或者仅仅是孩子的电子邮件账户使用列出允许的邮件发送方地址的方法对邮件来源进行过滤。

#### ⑤如果你使用了电缆 Modem、DSL、卫星或其他高速连接服务和设备

通常状态下,一直与网络相联的高速网络接入使家庭用户和小型商业非常容易被能在网络上以自动方式进行非安全连接搜索的探索软件捕获。即使某个系统安装了及时更新的防病毒软件和最新的补丁程序,智能化的探索软件依然能够在用户不知道的情况下侵入该系统。为避免此类秘密入侵,宽带连接(DSL、光缆、卫星或无线)用户应使用防火墙。

通过对防火墙进行设置,能够很容易地关闭计算机与网络相联的很多端口,仅保留用户所需的少数几个端口(如 E-mail 和 Web 浏览器)。借助防火墙,用户能够规定哪些程序可信并可以进入,而且还可以要求其他程序仅在得到许可后方能进入本系统。

#### (2) 在何处获得通用的网络安全建议

为帮助家庭用户与小型商业,政府机构、有关公司与非政府组织组成了“国家网络安全联盟”。该组织的站点([www.StaySafeOnline.info](http://www.StaySafeOnline.info))上有很多帮助信息和相关站点的链接。

#### 对于小型商业

小型商业中的工作人员可能希望由地方性项目或临近的社区学院或商务部门获得有关增强网络安全的好主意。国家级的联邦政府小企业管理局([www.sba.gov](http://www.sba.gov))和非营利性的国家小企业联盟([www.nfib.com](http://www.nfib.com))也能够提供必要的帮助。

在很多大城市,国家基础设施保护中心与地方商业团体、FBI 和学术界的专家共同成立了名为“Infragard”的组织([www.infragard.net](http://www.infragard.net))。该组织是一个在广泛的公共-私营部门联盟基础上的网络安全维护与网络犯罪防范组织。

在某些大都市,由美国安全服务机构赞助的公共-私营合作组织负责维护与金融研究院、信用卡和手机被盗事件有关的网络安全。这些团体被称为“电子犯罪防范小组([www.ussf.gov/ectf.htm](http://www.ussf.gov/ectf.htm))”。

此外,NIST 下属的计算机安全委员会建立了一个计算机安全资源站点([www.csrc.nist.gov](http://www.csrc.nist.gov))。该站点提供了与其他专业站点的链接。用户通过这些站点能够获得很多预警信息、软件更新信息和大多数常见的安全威胁清单。

#### 对于父母和教师

在以上所提到的提供过滤与教育信息的站点之外,其他一些能够帮助进行课程计划、为孩子提供有益帮助并帮助父母判断安全与否的站点如下:

“CyberSmart School Program”([www.cybersmart.org](http://www.cybersmart.org)): 专为教师提供课程计划与职业培训材料。

“NetSmartz”([www.netsmartz.org](http://www.netsmartz.org)): 用于指导孩子如何利用网络获取信息。

“Get NetWise”([www.getnetwise.org](http://www.getnetwise.org)): 为希望对如何考虑孩子上网问题进行决策的家庭提供网络资源。

由信息技术联盟赞助的“Cybercitizen Awareness”([www.cybercitizenship.org](http://www.cybercitizenship.org))向年轻人讲授网络道德规范和网络犯罪的风险。该站点也为教师、父母和年幼者提供材料。

工作安排	
第 1 级：家庭用户与小型商业	
建 议	
政府与非政府实体可采取的用于增进网络空间安全的具体行动	
R1-1	由于自动化的黑客程序能够对 Internet 进行扫描并找到未受保护的宽带连接，计划安装 DSL 或电缆 Modem 的家庭用户和小型商业应该考虑安装防火墙（某些 ISP 在为用户安装 DSL 或电缆 Modem 时提供防火墙软件）。一旦安装了防火墙软件，就必须定期访问该厂商的站点并对软件进行及时更新。
R1-2	每周都有新病毒出现，家庭用户和小型商业应确保运行及时更新的防病毒软件（某些防病毒软件提供商提供在线自动升级服务。某些 ISP 对所有接收到的电子邮件进行病毒扫描，随后才将它们发给用户）。
R1-3	新病毒通常以电子邮件的方式传播，家庭用户应在打开来自未知发送方的邮件（尤其是当这些电子邮件带有附件）时保持谨慎。为减少来自未知发送方的邮件，家庭用户应使用有关软件来拒收被称为“spam”的广告电子邮件（某些 ISP 提供能够使 spam 失效的程序。某些 ISP 提供允许用户拒收发送方不在朋友或者经选择的联系人之列的所有电子邮件）。
R1-4	为了增强计算机的安全，家庭用户也应通过访问厂商站点的方式定期更新各自的计算机操作系统（如 Microsoft Windows 和 Linux）和主要的应用软件（这些软件被用于进行 Internet 浏览或者创建文件、图表等）。（某些厂商提供在线自动升级）。
R1-5	ISP、防病毒软件公司和操作系统/应用软件开发商应该考虑进行合作，以便家庭用户和小型商业能够更便捷地获得安全软件（并且对其及时进行自动升级），包括有关软件升级与新补丁的警告信息。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	
行 动	
现有的网络安全工作	
1-1	为帮助家庭用户与小型商业，政府机构、公司与非政府组织组成了“国家网络安全联盟”。该组织的站点（ <a href="http://www.StaySafeOnline.info">www.StaySafeOnline.info</a> ）上有很多帮助信息和相关站点的链接。
P1-2	FTC 的“Guide for E-Consumers”（ <a href="http://www.ftc.gov/bcp/online/pubs/alerts/glblalrt.htm">www.ftc.gov/bcp/online/pubs/alerts/glblalrt.htm</a> ）
P1-3	FTC 的“How to Be Web Ready”（ <a href="http://www.ftc.gov/bcp/online/pubs/alerts/Webready.htm">www.ftc.gov/bcp/online/pubs/alerts/Webready.htm</a> ）
P1-4	FTC 的“How to protect Kid’s Privacy Online”（ <a href="http://www.ftc.gov/bcp/online/pubs/alerts/kidsprivacy.htm">www.ftc.gov/bcp/online/pubs/alerts/kidsprivacy.htm</a> ）
P1-5	在很多大城市，国家基础设施保护中心与地方商业团体、FBI 和学术界的专家共同成立了名为“Infragard”的组织（ <a href="http://www.infragard.net">www.infragard.net</a> ）。该组织是一个在广泛的公共-私营部门联盟基础上的网络安全维护与网络犯罪防范组织。
P1-6	Internet 欺诈诉讼中心（IFCC）是一个由 FBI 和国家白领犯罪中心（NW3C）组成的合作性组织（ <a href="http://www1.ifccfbi.gov/index.asp">www1.ifccfbi.gov/index.asp</a> ）。
P1-7	美国图书馆联盟“The Librarian’s Guide to Cyberspace for Parents and Kids”（ <a href="http://www.ala.org/parents/greatsites">www.ala.org/parents/greatsites</a> ）
P1-8	为帮助消费者获知通过 Internet 进行欺诈的事实、识别这些事实并在全美范围内与执法官员共享有关的法律诉讼信息，FTC、美国安全服务、FBI 和其他机构组建了“Consumer Sentinel”。（ <a href="http://www.consumer.gov/sentinel">www.consumer.gov/sentinel</a> ）
P1-9	美国司法部的计算机犯罪站点提供各种与计算机犯罪和计算机安全有关的信息，包括有关儿童的网络道德内容、邀请司法部进行谈话的链接。（ <a href="http://www.cybercrime.gov">www.cybercrime.gov</a> ）

续表

讨 论	
需要进一步分析、争议和讨论的重点问题	
D1-1	美国商业的最大组成部分是小型商业。通过 SBA，很多小型商业能够获得联邦政府的贷款。小型商业的网络状况对其雇员与国家经济的影响日益增大。应该要求那些寻求 SBA 贷款的小型商业通过一系列信息技术安全检查吗？
D1-2	父母和孩子如何建立针对家庭网络安全的对话？对于网络安全，父母和孩子有着各自不同的经验和专长。通过共享这些经验，家庭将能够改进其网络安全状况并对增进美国的整体网络空间安全状况做出贡献

6. 第 2 级：大型机构

本级的战略目标是鼓励并帮助大型机构建立安全系统。可以通过包括以下内容在内的自愿性行动实现该目标：

- 提升责任级别；
- 在适当的情况下建立负责网络安全的公司安全委员会；
- 实施 A.C.T.I.O.N.S.和最佳实践；
- 讨论无边界网络、大型机安全、即时消息和其他技术面临的挑战。

问题与挑战

能够支持美国的长期经济发展并对网络攻击具有抵御能力的网络基础设施的建立在很大程度上依赖于大型机构的安全。大型机构的网络运行不是孤立的，而是提供了驱动美国经济发展的常规性数据流。大型机构的网络所具有的抵御能力能够使美国在遭受网络攻击的情况下获得保护、检测、响应与恢复能力。只有通过大型机构运营商彼此间的合作，才能够获得可驱动国家经济发展的网络攻击抵御能力。

通过确保安全已构成了其网络体系结构、网络运行与管理的一个组成部分，大型机构在获得网络攻击抵御能力的过程中具有极其重要的地位。简化了美国经济运行方式的大规模网络既是国家强大的基础，但同时也使国家的经济发展具有脆弱性。

对于商务活动实施网络空间攻击的经济后果远非影响具体某个公司的近期运营情况，而是能够通过损害知识产权或敏感性的研究成果对宏观经济造成长期损失。不仅如此，安全脆弱性还能够使客户数据面临风险，侵害机构及其合作方的信心与信任关系。如果不加以补救，大型机构网络的脆弱性能够给该机构带来严重损失，并可能被利用，危害该机构范围之外的其他系统，甚至危害基础设施的安全。

网络空间安全是大型机构如今所面临的最复杂挑战之一。技术和政策挑战、全球范围的互联和基于 Internet 的商务活动都使企业安全的获得与管理复杂化。网络安全是一个变化和动态的目标。不存在可以实现机构安全的一劳永逸的解决方案或特殊技术。事实上，在目前的联网环境中不可能存在 100%的安全。

在机构范围内讨论网络空间安全不仅仅是一个技术问题，更多的是一个管理问题。网络安全所暴露的风险可以通过高层领导和机构董事会的参与得到管理。网络空间安全可能要求机构董事会的密切关注。仅在安全事件发生之后考虑安全问题将使企业的商业活动、客户甚至国家

面临风险。与之相对照，对于网络空间安全的有效监视则能够促进企业的发展、生产力和股东的信心。

## 战略讨论

### （1）提升责任级别

机构董事会在机构的结构系统中担任着重要角色，股东则拥有机构的所有权。机构董事会向股东负责，经理则向机构董事会负责。将网络空间安全责任提升到机构董事会的级别后，会在整个机构范围内产生显著的效果。通过询问一系列关于机构的安全结构与控制是否足够有效的问题，董事会能够更好地了解该机构的状况。为了更好地了解机构网络空间安全的规模、范围和有效性，某些董事会成员应该通过适当的董事委员会要求下属定期提交安全管理报告。

#### 公司董事会、金融分析师和投资者应该考虑的问题

- 哪些董事会成员负责信息技术安全与风险管理的监督？这些成员向董事会提交年度安全报告吗？
- 企业中负责信息技术安全的最高级别负责人是谁？他/她的直接上司是谁？
- CEO 与 COO 每隔多久对信息技术安全与企业整体的风险管理进行审查？
- 企业现有的信息技术安全政策是什么？企业是否为所有员工提供年度安全培训？
- 企业计算机系统的安全控制是否足够抵御非授权的文件访问、数据改动、交易秘密与资产的遗失或被窃？

美国商务部的关键基础设施保障办公室（CIAO）是负责与私营部门合作的机构，该机构将促使高级经理与部门主任意识到信息安全管理与保障的重要性。CIAO 与内部审计师协会（IIA）已经开始合作进行培训，以增强人们对在机构使命的意义下理解信息技术安全性重要性的认识。为了在全国范围内实现信息共享，IIA 与全美公司董事联合会（NACD）、美国注册公共会计师协会和信息系统审计与控制协会进行了合作。这些工作强化了机构董事会成员与高级经理对于他们在维护机构信息资产安全方面担负重要责任的意识。

### （2）成立公司安全委员会

目前各种各样的安全威胁要求人们进行新思考并采取新的应对措施。例如，某些大型机构可能考虑建立由机构内部承担安全相关责任的关键成员所组成的机构安全委员会。负责风险管理与承担安全相关责任的机构官员是该委员会的核心成员。这些官员包括：

- 首席运行官（COO）；
- 首席信息官（CIO）；
- 首席技术官（CTO）；
- 首席信息安全官（CISO）/首席安全官（CSO）；
- 首席风险官（CRO）；
- 隐私官；
- 负责物理安全的机构官员。

这些机构官员将通过整合现有计划，确保机构的网络空间安全被分解并加入到了机构的运行过程之中。由于网络安全维护过程中的一次失败即可导致机构的知识产权、客户信息和商业运行受损，关键决策的制定者和主要技术官员必须进行合作。不仅如此，他们还应在发生危机

的情况下为 CEO 提供建议，通过协调应急计划与持续性计划的执行对网络安全事件做出响应。大型机构对于网络安全的控制能力对于宏观经济甚至国家安全具有重要的影响。

### (3) A.C.T.I.O.N.S.与最佳实践

实现机构的完整性、可靠性、可用性和保密性可以采取的 A.C.T.I.O.N.S.有多种，详见下表：

A.C.T.I.O.N.S.与最佳实践措施

鉴别 (Authentication)	实施认证过程或程序，或者对网络用户进行验证，包括采用智能卡、安全令牌、生物测定或其组合的 PKI 技术
配置管理 (Configuration management)	在机构体系结构的计划与部署中考虑安全问题。进行配置管理，以便精确地了解所用的硬件、操作系统和软件（包括具体的版本号和补丁）；建立强健的访问与软件改变控制机制，责任分离；实施最佳实践；不使用默认配置
培训 (Training)	依据信息技术安全的需求培训所有相关员工，确保安全被分解并加入到了机构目前的运行过程当中。强化机构安全文化
事件响应 (Incident response)	锻炼机构对于事件响应、破坏程度减缓、系统恢复、计算机取证的调查与证据获取以及与执法机构进行合作的能力
组织网络 (Organization network)	为最大可能地利用有效的信息交换和机构知识，对机构安全管理、信息技术管理、风险管理功能进行组织
网络管理 (Network management)	建立对于网络脆弱性的定期的评估、修补、监视流程；考虑开发可用于脆弱性报告、为系统打补丁和检测内部威胁的自动程序。内部与外部的信息技术安全审计也可以用于进行网络管理
明智的采购 (Smart procurement)	确保安全被嵌入商业运行和支持该商业运行的系统中。这种安全嵌入方案比事后的弥补措施更易实施

### (4) 无边界网络

大型机构安全面临的最主要挑战之一来自于无边界的机构网络。对于网络与 B2B 商业运行模式的迅速采用改变了机构原有的边界定义明确的网络概念。如今，机构的互接程度非常密切，以至于当机构彼此进行合作时，具体操作人员可能都是些虚拟工作人员。虚拟工作人员指的是彼此通过网络进行交流，而业主并不知道这些人员的具体方位的机构工作人员。机构的管理计划不包括对于这些交流的记录，而这些交流通常发生在契约一方允许访问从属契约方的情况下。这种独特的交流方式正迫使机构安全管理发生着根本性的改变。这种改变又进一步要求针对安全管理进行新的研究、采用新的安全管理技术和新的安全管理方法。

### (5) 大型机

大型机将继续在大型机构中扮演重要角色。然而，一般安全策略和实践将主要被应用于笔记本电脑、网络服务器、网络设备、Internet 和普通性计算设备，而将大型机排除在外。大型机安全维护人员现在得到了新的机会，因为大型机技术和网络接入方式的改进带来了致使现有大型机安全策略与实践失效的新风险和新的脆弱性。不仅如此，合格大型机审计的频率与力度已经不再适用于新出现的威胁。组织和政府机构必须对其安全策略、安全实践与安全技术进行革新，使之切实有效并能够应对新的安全威胁。

### (6) 即时消息

即时消息程序给大型机构的系统带来了又一个脆弱性。例如，该程序能够绕过防火墙和病

毒扫描软件，允许恶意代码、非授权入侵的存在，以及允许重要数据在机构系统内部甚至机构外部的传输。机构应该调整其安全政策，以便应对即时消息程序所带来的风险。

#### （7）内部威胁

大型机构的系统上大约 70%的网络攻击来自可信的内部人员。这是具有对机构信息系统和网络进行合法访问权限的受信任人员。他们的某些行为可能对机构构成非常严重的威胁。内部威胁来源于恶意雇员的有意破坏行为，或者某个粗心的或安全意识不够强的雇员的无意行为。无论威胁的产生是有意还是无意的，结果是一样的，即破坏系统、致使系统瘫痪或造成数据丢失。有效防范内部威胁对安全策略、安全实践和持续性的培训均提出了要求。能够减少内部威胁的三个一般性策略包括：（1）访问控制；（2）责任分离；（3）有效的策略实施。

- 糟糕的访问控制会使个人或团体有机会为获取个人利益或者从事间谍活动而错误地修改、破坏或泄露敏感数据或计算机程序。
- 责任分离对于保护机构信息系统完整性具有重要作用。不应有人对一个系统享有完全的控制权。组织成员之间不正确的计算机责任分配将明显增加安全风险。
- 有效的机构安全策略实施极具挑战性，并且要求定期审计。新出现的自动化软件能够简化机构安全策略的实施。这些程序允许以人类语言的方式输入策略，将其翻译为机器代码，继而借助数据包的形式监视出入网络的所有数据传输。这类软件能够检测并阻止对于网络和基于网络的信息资源的错误使用。

级别 2：大型机构	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R2-1	CEO 应该考虑成立机构安全委员会，负责整体考虑本机构的网络安全、物理安全和可操作性。
R2-2	CEO 应该考虑采用常规的独立性信息技术安全审计、修补程序以及对最佳实践措施的审查。
R2-3	公司董事会应该考虑成立信息安全董事会委员会，应该确保 CEO 定期仔细审阅公司主要信息安全官员的建议。
R2-4	应定期审查和演练公司信息技术持续计划，应考虑站点和人员的更换。为消除风险，应考虑采用不同信息设备提供商的产品。
R2-5	公司应考虑主动参与业界活动，以便做到：（1）为同行公司开发最佳的信息技术安全实践措施和采购标准；（2）通过合适的信息共享和分析中心（ISAC）共享信息技术安全信息；（3）增强网络安全意识与对于公共政策问题的考虑；（4）与保险业进行合作，扩大保险在管理网络风险方面的作用。
R2-6	公司应考虑加入公共-私营部门合作组织，以便建立一个奖励计划，对为网络安全做出突出贡献的机构进行奖励。
R2-7	（1）机构应该审查大型机安全软件和程序，以便确保本机构利用了有效的技术和流程措施；（2）信息技术经销商和采用大型机服务器的机构应考虑进行合作，以便对大型机安全设备进行审查和升级，以及确保本机构继续拥有足够多经培训的主流产品应用领域内的专家；（3）信息安全审计应该包括对于主流产品的综合性评估。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	
行 动	
现有的网络安全工作	
P2-1	CIAO 与内部审计师学会（IIA）已经开始通过合作进行培训，增强对于在结合机构使命的意义下理解信息技术安全性的重要程度的认识。

续表

P2-2	国家威胁评估中心（NTAC）目前正在与 CERT 共同致力于一项针对本大型机构网络空间安全的研究。在早期研究经验（试验性案例研究项目和安全学校活动）的基础上，NTAC 希望建立一个对于安全威胁对机构信息技术安全的危害的更为全面的理解。具体信息见 <a href="http://www.survey.cert.org/InsiderThreat">www.survey.cert.org/InsiderThreat</a> ，可查看如何匿名参与该项研究的信息。
P2-3	Internet 安全联盟最近发布了“高级管理者意识指南”。该指南包括针对组织信息安全实践的 10 条最主要的建议。（ <a href="http://www.isalliance.org">www.isalliance.org</a> ）
P2-4	为了向各自的部门发布网络安全信息，很多关键基础设施工业已经成立了 ISAC。
P2-5	在很多大城市，国家基础设施保护中心与地方商业团体、FBI 和学术界的专家共同成立了名为“Infragard”的组织（ <a href="http://www.infragard.net">www.infragard.net</a> ）。该组织是一个在广泛的公共-私营部门联盟基础上的网络安全维护与网络犯罪防范组织
讨 论	
需要进一步分析、争议和讨论的重点问题	
D2-1	网络安全是一个要求进行定期评估与修补的持续性过程。因此，定期的信息技术安全审计能够增强网络安全。大型机构应以什么频率接受外部审计人员的网络安全审计？
D2-2	网络安全是公司运营的组成部分之一。当公司将网络安全列入管理问题时，它能够更好地保护其知识产权和商业运行。金融分析师与投资者应该在投资之前询问公司的哪些安全状况？
D2-3	大型机构能够以什么方式简化对于最佳网络安全实践措施的判定与实施？
D2-4	国家安全电信咨询委员会和国家基础设施保障委员会是否应考查建立一个独立组织的需求以及可能获得的益处？与独立的审计机构相类似，该组织将开发用于信息技术安全企业的安全标准、指南和审计程序

7. 第 3 级：关键部门

第三级之联邦政府

联邦政府的战略目标是显著提高联邦信息与信息技术的安全。为实现该目标，各机构都应该通过建立和实施由如下三个步骤组成的过程，以获得更好的安全性。

- 第一步：确定并记录机构的体系结构。
- 第二步：对威胁与脆弱性进行持续性的评估，理解它们对于机构运行和机构资产带来的风险。
- 第三步：为减少和管理这些风险，实施安全控制和矫正措施。

此外，为帮助私营机构实施如上三个步骤，下文的主要内容与过程将在联邦政府 IT 安全项目中通过如下行动得以实施：

- 进行预算和安全估计（由 OMB 负责）；使政府机构实现系统安全的可追究性。
- 更好地利用政府采购与集中化管理。
- 通过联邦政府部门信息系统安全委员会进行结构审查，以便确定、建议和协调联邦安全增强行动。
- 在联邦政府内部建立信息安全支持性服务办公室。
- 考虑是否需要开发用于独立的安全审查的专用准则；考虑是否应对合同方进行认证。

问题和挑战

联邦政府的安全由其各部局共同负责。联邦计算机安全面临威胁将给美国和美国人民带来



风险。

历史上，联邦政府从来没有系统地考虑过信息安全问题，而是经常将安全作为事后考虑——在威胁、脆弱性和攻击发生的情况下才做出反应，而非对它们进行预测并试图避免出现安全问题。

为克服这一缺陷，OMB 依据法律要求建立了一个政府 IT 安全项目。该项目可用来确立安全政策，并深入考查联邦机构是否满足安全要求。联邦各机构必须确保每笔投资中都有对于安全问题的投入，以此推进联邦政府的工作流程，而非不必要地阻碍这些机构行使其职能。

#### （1）联邦政府 IT 安全矫正过程

确保联邦信息技术安全性的关键步骤是了解各系统中安全与隐私控制的当前效果。一旦确定了该效果，还要实施连续性的风险评估，以始终跟踪系统的安全状态。长久以来，这一方法已经得到了 GAO 的推荐，并反映到了 OMB 的安全政策中，而且在 2002 年《政府信息安全改革法》（GISRA）中也得到了强调。

OMB 负责在联邦政府计算机安全项目中开发和监督政府的政策、原则、标准和指南的实施情况。在其法定的框架中，OMB 发布安全政策，并确保该政策能够与资金计划和预算指南相结合。监督基本上通过以下方式进行：预算与资金规划过程；独立的项目审查；年度机构项目审查；由总检查长（IG）实施的独立评估；机构提交给 OMB 的报告；机构安全改正行动计划；OMB 提交给国会的年度报告。

通过实施 GISRA，联邦机构必须对所有项目和系统进行年度安全审查，IG 将对机构的安全项目和子系统进行年度的独立评估。这些审查与评估可与其他应用安全审查一起确定机构在安全实施中的缺陷。为确保这些缺陷得到解决，机构必须为存在脆弱性的各系统与项目开发正确的行动计划。各系统的矫正计划直接关系到各机构为其系统申请的资金——OMB 掌管的系统资助项目可以投放给严重脆弱性矫正工作。此外，机构还必须确保其已经考虑了安全问题，并且在联邦资金规划过程中已经将安全向 IT 投资做了汇报。OMB 政策明确要求各项系统投资中必须包括明确的生命周期安全成本，否则将不予批准对整个系统的资助。各机构必须每个季度提交一份关于在弥补安全不足方面取得的进步的报告。OMB 每年要向国会提交对各机构进行安全审查的结果和 IG 评估报告。

年度审查能确定出系统的漏洞与脆弱性，并可最早揭示联邦政府间的 IT 安全不足。更为重要的是，通过制定和使用矫正计划，联邦政府已经建立了一个用来追踪脆弱性矫正工作进展的统一过程。

为确保安全能被作为一项关键的管理功能接受审查，年度状态报告将对管理层问题进行关注。OMB 与 GAO、各机构的 IG 以及其他专业机构均认为：合理的管理基础是必不可少的，它可确保重要的、但级别位于管理层之下的技术性安全细节得以充分地处理。矫正行动计划和每季度更新策略是联邦机构在了解了其具体的安全项目和系统的矫正工作状况后要作的工作。这些计划包括确定所有的管理性、运行性和技术性脆弱性，列出为矫正这些脆弱性所需的资源、进行矫正所需的时间以及矫正工作能否被跟踪。

#### （2）现有的不足与弱点

OMB 在 2002 年 2 月提交给国会的第一个关于政府信息安全改革的报告确定了政府各机构在安全表现方面的 6 项共同缺陷。

这些缺陷由来已久。OMB 与 GAO 和各机构的 IG 至少在 6 年前便发现过这些问题。评估

和报告 GISRA 中提出的要求的落实情况,使 OMB 和联邦机构可以开发一个崭新的、综合性的、能够在政府范围得以应用的机构 IT 安全表现基线。这些缺陷包括:

①缺少高级管理层的关注

高级管理人员必须持续性地建立并维护对于自己所负责的系统运行与资产安全的控制权。GISRA 指出,安全是一个必须由各联邦机构及其领导负责考虑的管理层职能。

②缺少对于行为绩效的评价

各机构必须对负责实施具体 GISRA 要求的官员的绩效进行评价。为了对机构的行为进行评估,机构必须对工作和项目的执行情况进行评价,即高级管理人员如何评价各级责任官员是否尽职?他们必须能够对负责机构运行与资产安全的官员的行为进行评价。事实上,在调查中,各机构对这一问题的反应表明其尚缺少对于 IT 安全相关工作与项目执行情况的审计机制。

③差劲的安全教育与意识培养

各机构必须增强安全教育与意识。一般用户、IT 专业人员和安全专业人员需要在对其上级负责之前获得为提高工作效率所需的知识。

④未能在资金规划与投资控制中充分考虑安全问题

安全必须通过有效的资金规划与投资控制被融入到各个系统与项目当中。正如 OMB 在过去两年的预算指南中所要求的,联邦各机构要就安全投资的情况进行报告。没有在 IT 资产规划中考虑安全问题的系统将得不到资助。

⑤确保契约服务具有足够的安全性

由于多数联邦 IT 工程由合同方负责实施和运行,各机构必须确保合同方的服务足够安全。因此,包括电信在内的 IT 契约需要具备足够的安全要求。很多机构的报告显示,合同中尚缺乏安全控制的内容,或者无法对合同方是否实现了必要的安全要求进行验证。另外,OMB 报告还讨论了目前在很多商业软件产品中发现的普遍缺陷。这些缺陷本身不影响软件的效果,但却对安全不利,现在必须在全国范围内讨论这一问题。

⑥未能检测、报告并共享脆弱性信息

很多机构并没有可用于测试的系统或没有监视系统的运行情况。因此,它们无法检测到入侵行为、可疑的入侵和病毒感染。由于响应工作要依赖于检测,各联邦机构的系统及运行面临着巨大的风险。最糟的结果是在没有检测并报告 IT 安全问题的情况下导致了灾难性毁坏。美国的众多网络互联环境意味着安全状况最好的系统与安全状况最糟糕的系统共同分担着安全风险。

对整个联邦的提早预警要通过其中某个机构的检测开始,而不是位于 FBI、GSA、DoD 等处的事件响应中心。这些事件响应中心仅是保存着经他人报告得来的信息。报告只能由检测得来,矫正工作要同时依赖于监测和响应。因此,这一需求不是一个技术问题,而是一个管理问题。此外,非常关键的一点是,各机构及其组成部门应及时将所有安全事件报告给 GSA 的联邦计算机应急响应中心和适当的执法部门(如 GISRA 所要求的 FBI 下的国家基础设施保护中心)。

以下是其他的问题和挑战。

(3) 鉴别:网络安全的关键

通过伪装为合法用户获得系统访问权限的入侵者具有极其严重的破坏力。依据 NIST 的《计算机安全介绍——NIST 手册》(见 [www.csrc.nist.gov](http://www.csrc.nist.gov)) 的描述,有三种确保用户标识与鉴别的

基本方法：依据用户已知的某种事物（如口令）；依据用户拥有的某种事物（如令牌或智能卡）；依据用户自身的某些特征（如生物信息）。强度最弱并且最常见的方法是第一种。该方法的强度最弱，因为可能的入侵者通常能够成功地通过与不知情的用户的对话和相对简单的技术手段获得口令。

如果一个入侵者能够获得某个机构成员的口令，他就能获得该成员的访问权限并在防火墙后运行，从而可以使用和影响系统资源，并对敏感数据进行实时访问。此外，该入侵者或许也能够访问同一域中的其他系统。

如果这个机构成员具有管理员权限或高级用户权限，入侵者就将获得这些权限并不受任何约束地访问整个网络及其上的全部信息。更糟糕的是，该入侵者还能够获得重要信息，并掌握系统的漏洞，还可在无法被检测到的情况下离开，并在未来的某一天再次入侵该系统并造成更为严重的破坏。

#### （4）不一致的应急计划

由“9·11”事件之后进行的安全审查所得到的教训表明，联邦机构的通信及其他网络的应急能力具有严重的不一致性，并且大部分应急计划不完整。应急计划是维护网络空间安全的关键因素之一。缺乏充分的应急计划和培训，联邦机构便无法有效应对其服务遭受干扰的情况，也无法确保机构业务的继续正常进行。应急计划必须接受测试，以便确保机构雇员能充分意识到各自的分工与责任。

#### 战略讨论

为充分理解 GISRA 的意图，联邦政府必须采取综合性的方法来增进网络空间安全状况。很显然，没有一劳永逸的网络安全解决方案。然而，以下三个因素对于联邦政府实现和维持强健的网络空间安全至关重要：

- 标识并记录下整个机构的体系结构。
- 对威胁与脆弱性进行持续性的评估，理解它们对于机构运行和资产带来的风险。
- 为减少和管理这些风险，实施安全控制和矫正措施。

#### （1）第一步：确定并记录下整个机构的体系结构

作为 OMB 政策的一部分，各机构必须确定并记录其整个体系结构，包括制定一个权威的清单，记录下所有的操作和资产、所有的 IT 系统、所有的关键业务运行流程及其与其他机构的相互联系。该清单将使政府充分了解其安全需求。联邦政府目前正在将 OMB 与联邦 CIO 委员会的政府机关体系结构活动以及关键基础设施保障办公室的 matrix 项目相结合，目的在于更好地确定并记录各机构及跨政府的核心过程、不必要的重复域以及缺少必要冗余的领域。对跨机构的业务运行过程中潜在的威胁与脆弱性进行的建模与评估也将从上述工作中受益。

#### （2）第二步：对威胁与脆弱性进行持续性的评估，理解它们对于机构运行和资产带来的风险

商业化的自动审计与报告机制目前可用于认证系统中的安全控制，并可持续性地理解这些系统中存在的风险。某些民间机构已经增加了对于这些系统的使用，其他更多地机构也应如此。因此，联邦政府将推广对于自动化工具的有效应用，将其用于检测入侵、定期进行脆弱性评估、积极管理并减少威胁，以及持续性地审计 IT 系统的安全状况（见建议 R3-5）。

由于各机构增加了对于自动化工具的使用，联邦政府将会考查采购、运行和管理这些工具是否可以带来某种益处。一个可能但非唯一的方法是由 FedCIRC 负责对这些工具进行集中部

署和管理。该方法能够使脆弱性的标识与报告实现标准化和自动化——这是 OMB 提交给国会的 2002 年 2 月的安全报告中确定的六个主要缺陷之一。

联邦机构的网络上的自动化工具能够对系统脆弱性进行持续性的评估，并收集和分析防火墙和入侵检测日志，对安全配置与安全策略控制进行审计，并自动向 FedCIRC 报告审计结果。自动化工具可以帮助进行数据分析、提供前瞻性的评估。并对机构运行无法接受的风险进行预警。

同时，各机构及项目官员应继续对其控制下的运行安全与资产负责，并有义务向上级负责。这种责任与义务的分离会使他们误以为安全与其无关，但事实并非如此。在采取任何集中管理方式之前都必须进行慎重考虑（见建议 R3-6）。

### （3）第三步：为减少和管理这些风险，实施安全控制和矫正措施

实施能够将风险维持在可接受级别上的安全控制，并确保这些控制的有效性而对其进行测试，这通常能够在短时间内完成。然而，对脆弱性进行矫正非常复杂。软件会经常发生改变，每次升级都会带来新的脆弱性，因此必须对脆弱性进行持续性的评估。矫正的方法通常是打补丁，或安置对主要程序进行升级所需的软件或代码。此外，联邦政府应该在开发和评估可能会为机构运行带来益处的实施方案时，应该采用更为安全的网络协议。当这些安全协议能够为机构的运行带来较好的成本效果时，联邦政府应该带头采用它们。

### （4）对用户进行标识和鉴别并维护授权

通过电子政府的 e-Authentication 工作及其他手段，联邦政府正在逐步获得所有联邦雇员和过程的连续性安全链，包括在适当的场合使用生物智能卡进入建筑物或访问计算机、在用户登录计算机时进行用户身份鉴别。这种做法的益处显而易见。为建立并维护安全的系统运行，联邦机构必须确保系统中的用户具有他们所宣称的身份，并且确保这些用户只能够做经允许的事情。

对系统用户进行标识和鉴别是系统安全链的第一个环节。目前所用的很多鉴别程序是不充分的，甚至配置正确的用户口令也能够被他人使用。然而，依据 GAO 和其他报告，用户通常并不去改变系统设置的默认口令，用户口令的设置通常有误，并且用户很少对其口令进行更新。

通过进行综合采用强口令、智能令牌和生物技术的多层次标识与鉴别，联邦政府将消除很多目前存在的显著安全问题。通过正在进行的 e-Authentication 行动，联邦政府将审查对于强访问控制和鉴别的需求；扩大所有能够采取相同的物理与逻辑访问控制工具和鉴别机制的部门的范围；进一步促进部门间的一致性与互操作性。

### （5）系统配置管理

通过 PCIPB 的行政部门信息系统安全委员会和政府范围的体系结构开发活动，OMB 正寻求在联邦机构范围内获得更好的系统一致性的方法以及能够通过安全过程进行简化和一致化来增强安全效率和效果的方法。

通过预算过程，联邦政府将鼓励各机构对商业自动化工具进行投资，从而帮助它们确保能对各异的体系结构和系统配置进行正确维护。正如联邦 CIO 委员会的《联邦体系结构实践指南》中讨论的，配置管理对于体系结构维护非常关键。CIO 委员会的指南见 [www.itpolicy.gsa.gov/mke/archplus/ea\\_guide.doc](http://www.itpolicy.gsa.gov/mke/archplus/ea_guide.doc)。

该指南也描述了对于将定期配置审计作为这一体系结构的控制特色的需求。目前有很多商用的自动化工具均可实现这类审计。配置控制对于安全性有着偶发但重要的意义，即控制系统配置允许机构在整个系统或网络范围内以更有效、更经济的方式实施安全政策和授权，同时也

进一步简化了防病毒软件的安装和其他软件的升级与打补丁过程。

#### （6）政府外包与采购中的安全性的提高

通过 OMB 的联邦采购政策办公室、联邦采购规则委员会和联邦机构信息系统安全委员会的合作，联邦政府正在试图确定能够增进机构合同安全和评价整体联邦采购过程安全的方法。对外

包工作中的安全的维护是 OMB 在其 2002 年 2 月提交给国会的报告中所确定的最主要的安全缺陷之一。

此外，联邦政府正在对 NIAP 进行综合审查，目的是确定 NIAP 能在多大范围内解决商用软件中的安全缺陷。审查内容将包括在实施国防部 2002 年 7 月发布的政策后得来的经验教训。该政策要求政府

#### 国家信息保障联盟 (NIAP)

美国政府建设 NIAP 的目的是满足 IT 产品的厂商和消费者对安全产品实施测试、评价和评估的需求。NIAP 是国家标准与技术研究院 (NIST) 与国家安全局 (NSA) 在实施 1987 年《计算机安全法》规定的各自职责的过程中联合建设的。

这一联盟于 1997 年建立，它综合了上述两个机构在网络安全方面的经验，就 IT 产品和系统在网络安全方面的技术需求以及对这些产品的评估方法开展了研究。NIAP 的长期目标是通过成本有效性合理的测试、评价和评估项目增强消费者对信息系统和网络的信任。NIAP 将在多个领域继续与政府部门和工业界建立密切的合作关系，旨在帮助解决当前或未来可能对国家信息基础设施造成影响的安全问题。关于该联盟的更多信息可以参考 <http://www.niap.nist.gov>。

采购经 NIAP 或其他类似评估过程认证过的产品。该政策强调指出，如果一类产品中有的产品通过了评估，则 DoD 的单位必须采购这些经评估的产品。如果目前还没有通过评估的产品，则 DoD 的单位必须要求未来的经销商提交其产品时接受评估，以便考虑是否采用该产品。

经过这一过程，联邦政府将评估把该过程扩大至所有联邦机构的成本有效性。如果可行，它不仅将增强政府网络空间的安全，而且将最大可能地优化政府的购买力，从而影响市场，提高、改进所有消费者 IT 产品的安全性。联邦政府意识到，过去的很多类似努力都失败了，但是政府相信，政府与消费者对 IT 产品缺陷的不断关注将推动未来的新的类似工作。

#### 战略框架

##### （1）采用机构负责制

在当政初始，布什总统曾号召加强联邦政府的管理。自 2001 年 2 月的预算蓝图开始，到 2002 财年与 2003 财年的预算中，以及在其管理改革日程中，布什总统均重申了清晰的政府改革日程，下令通过五项政府级的行动来共同推进政府来实现更好的改革效果，可见 [www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf](http://www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf)。由于建立并维持一个有效的安全项目是稳固管理的基础，联邦政府正在采用总统的管理日程计划来建立其工作基础，以推动安全项目的改革。

管理日程计划中的行动之一——扩大电子政务激发了对信息技术与网络的利用并提高了政府的工作效率。本战略将通过确保电子政务行动及其所依赖的基础设施的安全性来对这些工作进行补充。联邦政府将更为积极地对威胁与脆弱性进行预测，尽可能消除它们，并在不可能消除它们的情况下保护自己。这样，联邦政府将成为国家关键基础设施的全部所有者和运营者的榜样。

良好的目的和好的开端并不是这一行动成功的关键。政府需要的是效果。为明确责任并衡量工作效果，政府将做以下三件事。

- 分析联邦机构的安全绩效证据，评估该机构对政策的遵循性。GISRA 要求联邦机构对其信息安全项目与实践进行独立的年度评估并向 OMB 报告评估结果。这些报告包括机构内的系统与项目中所有的安全缺陷以及带有具体阶段性目标和时间表的安全状况改进计划。这些报告将同预算过程相结合。该机构向 OMB 提出的信息技术资助请求必须考虑安全的生命周期代价，否则该请求将不被批准。OMB 将利用这些数据对机构的安全运行情况进行评分。OMB 的首轮安全报告已经在 2002 年 2 月提交给了国会（[www.whitehouse.gov/omb/infoereg/fy01securityactreport.pdf](http://www.whitehouse.gov/omb/infoereg/fy01securityactreport.pdf)）。
- 利用管理“评分表”评价联邦机构的进步。对总统发布的每个管理日程计划，OMB 均采用了行政部门管理“评分表”，即一个目前在商业界普遍使用的简单的“交通指示灯”分级系统。“绿色”代表机构业务的运行是成功的，“黄色”则代表了多种混合结果。在电子政府的“评分表”中，OMB 便以此来评价各机构安全状况（[www.whitehouse.gov/omb/memoranda/m02-02.html](http://www.whitehouse.gov/omb/memoranda/m02-02.html)）。
- 对于联邦机构的资金决策以该机构的网络安全状况为基础。在随后的 3 年时间里，联邦政府可能在 IT 安全（包括研究和开发）上投资 200 亿美元。OMB 将在对各联邦机构的 IT 资助请求进行预算决策时继续同时采用“评分表”和 GISRA 的安全报告制度。OMB 的政策非常明确：对于安全状况糟糕，或者在其 IT 资助请求中未考虑生命周期代价中的安全问题的联邦机构，其资助请求将得不到批准（[www.whitehouse.gov/omb/memoranda/m00-07.html](http://www.whitehouse.gov/omb/memoranda/m00-07.html)）。

这些评价将有助于确保各机构通过开发并维持其稳固的安全管理的途径改进和维护整个联邦政府的安全状况。联邦机构的运行与技术性安全控制均建立在其安全管理的基础之上。管理基础则包括：进行明确并且无二意性的安全职责分配；在责任履行上采用官员负责制；在预算与资金使用计划过程中结合考虑安全要求。

#### （2）成立信息安全支持性服务办公室

“建立一次，使用多次”的方法要求由一个中心机构来负责管理并资助某些安全工作。另外，信息技术日益增加的复杂性正在给很多机构（尤其是小规模机构）造成明显压力，迫使它们开始讨论各自的安全要求。对于联邦民事机构，国土安全部下设的一个办公室能够执行这些支持功能。该办公室将在 OMB 的目标指导下运行，办公室中包括来自其他机构的资源，并能够帮助 OMB、NIST、CIAO 和其他一些机构承担其责任（建议 R3-9）。

#### （3）联邦网络空间事件响应计划

总统关键基础设施保护委员会下设的事件响应委员会正在扩展由 FEMA（[www.fema.gov/rrr/frp/frpintro.shtm](http://www.fema.gov/rrr/frp/frpintro.shtm)）负责维护的联邦响应计划（FRP），在其中加入对网络空间事件的响应。FRP 已建立了一个有关过程和组织结构，用于系统地、协调并有效地实施联邦服务，以便解决《Robert T. Stafford 灾难救济和应急救助法》中所谈到的大规模灾难或紧急事件。EPR 扩充后将在发生大规模网络威胁或攻击的情况下确定领导机构的角色、职权和联邦网络响应管理政策。该文将以附件形式提出一个综合性的应急计划，详细描述联邦政府应如何对大规模网络事件做出响应。

当前工作的一个重要的副效应是使事件响应能力朝着更加高效和协调的方向发展。改进后

的能力中的一个关键组成部分是显著增强的分析和预警能力，包括由事后分析观点向事前预测观点的转变。联邦政府目前正在加强和统一各机构针对其通信网络和信息系统所制定的偶发事件与灾难恢复计划。

#### （4）安全战备实践

为了对民事机构的安全战备状况和应急计划进行测试，联邦政府正在考虑采用基于演习的行动来评估某个威胁对于选定的跨政府业务过程的影响。一个可能的方法包括在政府范围内进行网络空间安全演习。该方法与国防部 1998 年在“合法接收方（Eligible Receiver）”行动中所采用的方法类似，并且将通过各参与机构的合作得到发展。演习将涉及包括物理、运行、信息和系统在内的绝大多数安全原则。演习中，将查看这些面向具体机构的演习和独立测试是否能够揭示低概率事件对互联系统和过程造成的严重影响。演习中发现的脆弱性将列入机构的 GISRA 矫正计划中（建议 R3-8）。

#### （5）尝试建立一个独立的联邦通信与信息系统基础设施

联邦政策正在强调各机构必须规划并提供包括通信在内的操作持续性。这一计划和服务支持应该在政府内部保持一致，希望创建新职能的联邦部局应该首先审查跨机构间的共享协议。

联邦政府将评估在服务中断时各种应急替代方案的可行性和成本有效性，如 VPN、专网等（建议 R3-6）。

#### （6）为独立的安全审查和认证而开发专用标准

随着安全重要性的日益增加，对于机构的安全项目与措施的独立检验和认证的需求也在增大。GISRA 和 OMB 的实施指南中均要求联邦机构的项目官员和 CIO 至少对其项目的安全性进行年度审查，但很少有联邦机构能拥有合格的审查人员，因此他们经常把该项工作承包出去。

联邦各机构和 OMB 已经发现，承包商的安全专业水平参差不齐，既有真正的专家，也有难以令人满意者。此外，很多独立的认证承包商同时也在从事安全项目的实施工作。因此，它们对于项目的审查将带有个人偏好。事实上，OMB 在 2001 年已得知一些安全服务提供商被实施项目时同样的机构邀请进行年度的 GISRA 项目审查。在对某个联邦机构的网络空间安全情况进行评估时，应该避免涉及利益冲突方。

联邦政府将确定是否应要求联邦政府的安全服务提供商——私营部门通过某种最低的能力度的资格认证，包括认证这些私营部门的独立性。国家安全界已经开始对在敏感环境中工作的安全服务提供商进行此类资格认证。所获得的经验将被用于考虑将该方法在应用于其他联邦政府领域时成本有效性。

该方法的内容之一是对满足具体的公开性准则的服务提供商颁发营业许可。这些准则的内容既涉及安全专业级别（包括这些服务商对所有的政府要求具有透彻的理解力），也涉及服务提供商的相对独立性。为确保独立性，机构必须避免雇用其现有的（甚至先前的）安全服务承建商进行该机构的安全项目审查工作。

计划中所有这些建议均不会危害 GISRA 下设的各联邦机构总检查长的职责。OMB 将继续视总检查长为促使机构改进其安全运行情况的主要力量。事实上，总检查长将直接通过实施该计划获益，即从中获得进一步的独立性和专业性信息（建议 R3-2）。

#### （7）由 PCIPB 的行政部门信息系统安全委员会实施的高级审查

除前述的行动外，OMB 委员会还正在对很多安全问题进行审查，以通过保障各机构的运行而获得更大的收益。为了了解安全政策对于各机构项目与业务运行所产生的影响和作用，该

委员会的成员包括了来自联邦政府很多部门和机构的官员：首席信息官、首席财务官、总检查长、采购执委、小机构、运行性项目官员、人力资源官员和预算官员。

该委员会当前以及计划中的活动包括对目前政策与过程的缺陷分析、对政府范围内通用风险等级划分方法可行性的评估，以及审查是否需要为相似的运行过程、资产和系统开发一致的安全措施和基准。其中，后两者体现了“建立一次，使用多次”方法。

#### (8) 当前政策与过程的缺陷分析

需要审查目前非国家安全应用中的 IT 安全政策、标准和指南是否存在缺陷，具体内容包括：它们是否能在具体的细节和所涉及范围上满足联邦各部门与机构的需求，并且能帮助各机构去增进其安全实施状况？考虑到现有政策在所有相关机构与组织中的具体应用情况，这些政策的开发过程是否需要保持高效并且有效？在需要改进的情况下，委员会将提供适当的建议。

#### (9) 划分风险等级

对联邦各机构和其他组织目前的风险评估实施活动进行审查，并判断是否需要制定一个适用于所有机构的风险等级划分的统一策略。业已开始考虑的一个问题是：在政府范围内采用通用方法（如用于确定高级、中级和初级风险暴露情况的具体矩阵）是否能够降低复杂性，简化基于风险的安全控制工具的使用，并且增进不同机构彼此间的互操作与信息共享？

#### (10) 对于类似的运行过程、资产和系统采用统一的安全措施或基准

PCIPB 将考查针对前述的风险定级工作中划分的高、中、基本三类风险等级的应用，是否有必要制定统一的安全措施，以及制定统一措施所能带来的益处。委员会将研究在不同联邦部门与机构中对业务运行的安全实施、维护和监视是否能够减少成本并增加类似这些运行的安全性。

这项工作中还将对若干假设进行测试。首先，很多机构的项目和 IT 运行情况在本质上是相同的（如电子邮件、Web 服务器、金融系统、通用支撑性系统或网络），并且具有基本类似的安全要求。其次，集成了所有可适用的安全策略和技术指南的统一安全措施将简化，并缩减类似活动中的安全成本。最后，统一的安全措施在风险划分等级得以统一后要具有可行性。

#### (11) 整个政府范围应采取的步骤

上述的大部分内容的一个共同目标是统一并简化安全项目和过程，以及在整个政府范围内实现安全的一致性。这种用来实现政府安全的“建立一次，使用多次”的方法与电子政府行动和 OMB 为各机构下发的 2004 财年预算请求准备指南保持了一致。OMB 指南指出，OMB 将优先考虑那些跨政府实体的大规模技术采购行为。有关 OMB2004 财年预算指南的具体内容见 ([www.whitehouse.gov/omb/circulars/a11/01toc.html](http://www.whitehouse.gov/omb/circulars/a11/01toc.html))。

保护国家基础设施的一个主要目的是确保存在一个国家环境——包括人、过程和技术，以在联邦政府、地方和州政府以及私营部门之间实现重要的反恐信息的整合。我们必须拥有一种能在任何时间均能够为正确的人提供正确的信息的信息的机制。通过采用信息技术，美国各地的国土安全官员将能

#### 用于国土安全的信息整合技术

为指导信息整合，总统建议在商务部的关键基础设施保障办公室下成立信息整合项目办公室 (IIPO)。该机构一旦建立，则将移归国土安全部。它负责协调全国的关键信息的共享。它的主要职责是设计并帮助实施一个国家级的体系结构，以此指导对于信息技术的投资和应用。该体系结构将在缩减响应时间和提高决策质量的情况下，定义在美国和全球范围内检测、预防、监视和响应恐怖分子威胁与恐怖事件所需的信息集成要求。



够对威胁和脆弱性获得完整和共同的认识，也能够获知可被用于减缓这些威胁的人员和资源情况。这些官员将从各级政府和私营部门那里获得所需信息，以便预测威胁并迅速有效地对其做出响应。对这类信息的整合将促使这些官员更好地保护物理和网络基础设施、保护美国的国家边界、预防生物或化学攻击，并在第一时间对恐怖分子或自然灾害事件做出有效响应。

#### ①主要战略目标

- 在州和地方政府以及私营部门之间建立稳固的合作。
- 确保采用领先的信息技术并将其作为预防和检测恐怖主义活动的防御性武器。
- 推动国家与国际信息集成与信息传输标准的形成。
- 开发新的服务交付模型与业务运行模型，使政府能够使用所获的政府范围之外的信息。

#### ②当前目标

- 在联邦机构范围内实现对国土安全至关重要的信息的整合（横向整合）。
- 在联邦、州和地方政府以及私营部门之间促进对国土安全至关重要的信息的整合（纵向集成）。
- 通过正确使用信息技术、产品和服务，指导国土安全国家战略的实施。

#### ③待解决的主要风险

- 在增强安全的同时维护隐私。
- 制定合理的政策与法律。
- 在文化信仰与多样性方面进行均衡。
- 整合重复性的工作。
- 克服政治和文化障碍。
- 针对新技术确保适当的安全措施。

#### ④在建议性的信息整合战略中的主要工作

- 开发一个业务驱动的国土安全体系结构。
- 实施国家的国土安全信息港湾（即其 Web 站点）。
- 密切关注联邦“监视”列表中的内容。
- 各州之间共享执法信息。
- 建立一个数字化的国家国土安全信息中心。
- 将数字化智能代理用于预防和检测恐怖主义活动。

工作安排	
第 3 级：关键部门——联邦政府	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R3-1	以增强对更安全的产品的采购为目的，联邦政府将在 2003 财年第四季度之前完成对国家信息保障计划（NIAP）的综合考查，以便做到：确定 NIAP 的成本有效性并找出其中的安全不足；判断 NIAP 是否为消除这些安全不足而确定了发展目标，是否正在试图实现这一目标，并判断 NIAP 的改进、优化、扩充工作的适宜性及成本有效性。
R3-2	在 2003 财年第三季度结束之前，联邦政府将确定是否应该要求为联邦政府提供安全服务的私营部门通过某种最低能力程度的资格认证。

续表

R3-3	通过采用电子政务模型，在 2003 财年第三季度结束之前，联邦政府将通过在政府内部更广泛地采办、运行和维护安全工具与安全服务而获得益处（包括减少小型机构的资源压力）。
R3-4	通过正在进行的 E-Authentication 行动，在 2003 财年第二季度结束之前，为促进部门间的一致性与互操作性，联邦政府将扩大所有能够采取相同的物理与逻辑访问控制工具和鉴别机制的部门范围。
R3-5	联邦政府部门应该继续扩大自动化的机构安全评测和安全政策实施工具的应用程度，并为免受攻击而积极采用威胁管理工具。2003 财年第二季度结束之前，联邦政府将针对是否有必要采取具体行动以便进一步促进这些工具的使用进行决策。
R3-6	联邦政府将评估在服务中断时各种应急替代方案的可行性和成本有效性，如 VPN、专网等。
R3-7	联邦政府应该带头采用安全网络协议。联邦政府应该在安全协议发布之初即考虑该协议是否消除了某个安全脆弱性，以及该协议的应用是否能够对联邦政府的网络运行和安全状况产生性价比合理的影响。
R3-8	2003 财年第二季度结束之前，联邦政府将选择一个机构，考查安全和应急战备演习的成本有效性。演习中发现的脆弱性将列入机构的 GISRA 矫正计划中。
R3-9	OMB 将与 CIO 委员会进行合作，在遵循事实的基础上确定是否应该为整个联邦政府的安全测量而成立一个领导机构。可供选择的现有机构包括 GSA、NIST、国土安全部、国防部。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	
行 动	
现有的网络安全工作	
P3-1	国家安全局： <a href="http://www.nsa.gov/isso/index.html">www.nsa.gov/isso/index.html</a>
P3-2	国家基础设施保障联盟： <a href="http://www.niap.nist.gov">www.niap.nist.gov</a>
P3-3	OMB 安全项目/预算项目/GISRA 报告： <a href="http://www.whitehouse.gov/omb/inforeg/infopoltech.html">www.whitehouse.gov/omb/inforeg/infopoltech.html</a>
P3-4	电子政务行动： <a href="http://www.egov.gov">www.egov.gov</a>
P3-5	联邦体系结构项目矩阵： <a href="http://www.ciao.gov/Federal">www.ciao.gov/Federal</a>
P3-6	NIST 计算机安全资源中心： <a href="http://www.csrc.nist.gov">www.csrc.nist.gov</a>
P3-7	联邦 CIO 委员会： <a href="http://www.cio.gov">www.cio.gov</a>
P3-8	GSA 的 PKI 桥和联邦通信系统安全级： <a href="http://www.gsa.gov">www.gsa.gov</a>
	联邦计算机应急响应中心： <a href="http://www.fedcirc.gov">www.fedcirc.gov</a>
讨 论	
需要进一步分析、争议和讨论的重点问题	
D3-1	是否应要求联邦机构制定用来安装针对已知脆弱性的补丁程序的最长时间？
D3-2	CIAO 或 CISO 是否应该与 CIO 具有不同的职责？
D3-3	民事机构应该如何扩大在具体场合中的 PKI 应用？

### 第三级之州和地方政府

州和地方政府已经设立了各自的战略目标，以实现和维持其保护关键信息基础设施的能力，防止那些有可能严重削弱州和地方政府的治安和关键性社会服务能力的自然事故或人为事件发生。

#### 问题和挑战

美国各州提供的服务构成了数百万美国人民的“公共保安网”。这些服务包括重要的社会

保障活动以及关键性社会保安职能，如执法和应急响应服务。各州还拥有并运营着很多关键基础设施系统，如电能和传输系统、运输系统、供水系统等。它们扮演了一种催化作用，能够把州内提供各项关键服务的各方召集到一起，共同对发生的危机进行防备、响应、管理，并从危机中实施恢复。在我们的联邦系统中，州政府提供的关键服务使其担负着特殊的角色和责任，使州政府因此而成为了一个关键基础设施部门。

由州政府实施的很多这样的关键职能都必然地与 IT 紧密相连，包括福利金的提供、因执法目的而以电子手段访问犯罪记录、州政府的公共事业和运输服务的运转。我们要能够阻止攻击，或在攻击事件发生时迅速响应，这样才可确保这些服务能全天可用，才可提供公众所期望的关键服务。

IT 系统使州政府具有了前所未有的效率和响应能力。公民对这些 IT 系统以及这些系统上收集并存储的数据的完整性所持的信心是很重要的，它能使这些 IT 系统的优越性得到进一步的体现和充分利用。

#### 战略讨论

随着对集成系统的不断依赖，州、地方、联邦机构不得不联合起来对付网络攻击。系统保护信息的共享对于确保政府的连续性来说是很重要的基础。各州已经采取了很多机制来促进对网络攻击信息的共享以及对攻击事件的报告。当新的政策出台以及新的技术解决方案出现时，这些机制还在不断地更新和改善。除此之外，州政府正在探索某些方法来改善对内、对外的信息共享。这些方法包括以立法的形式为网络安全提供进一步的资金和培训项目，还包括在州、地方、联邦政府之间组建合作联盟来共同对付网络威胁。

被多个州政府用来解决网络空间安全问题的机制包括：

- 政府架构。很多州政府已经建立了 IT 安全政府架构，用来指导和颁布本州内的网络安全策略。其功能包括为州长制定策略建议，并建立恢复优先级列表，以应付政府的多个机构同时瘫痪时出现的局面。很多州的实例中，网络安全委员会包括了政府和有关机构的所有部门。此外，某些州的架构中还包括地方政府，因为它们意识到了地方系统与州系统的互联性。
- 设立州首席信息官（CIO）和首席安全官（CISO）角色。CIO 和 CISO 将负责检查安全策略，监督关键信息系统的实现和维护。
- 州政府的国土安全活动。国土安全主管领导认为，州政府的网络系统对恐怖分子的袭击呈现高风险性。因此，州政府正在加强其网络基础设施，并在州信息系统中实施了鉴别和授权过程。各州的策略制定者以及技术专家正在向公众做推广工作，以教育他们如何去保护自己位于家中的信息系统。

#### 执法

州和地方政府在应急执法领域担当着重要角色。作为一个关键基础设施部门，应急执法服务（ELES）是应急服务部门的一部分。在危机时期，ELES 部门的连续性运行对于法制、公共福利保护、公民自由和隐私权的保护以及后果管理都十分重要。

对不足的分析

一些州内的代表组织已经确定，但为了发展政府间以及工业界的合作联盟，还需要如下机制：

- 建立州 CIO 咨询集团，对总统关键基础设施保护委员会负责。
- 创立一个跨政府、跨学科的体系结构设计指导方针，以支持国家范围内的信息共享。
- 进一步加强信息共享工作，如各州之间的信息共享和分析中心。
- 发起一项持续性的政府间工作，在与 NIST 的合作下，为州和地方政府开发并向其交付网络安全工具和培训材料。
- 对于处在不便获得网络安全知识和工具的区域中的公民和企业，实施协调一致的推广工作。
- 确保地方政府的代表能参加州政府的网络安全委员会，以使地方的利益和需求得到体现。
- 权衡从私营工业安全提供商处得到的最佳实践措施、趋势、教训和新技术。 寻求能够在各级政府的信息孤岛之间建立沟通桥梁的途径。
- 解决州政府的信息共享问题。

ELES 部门由超过 18 000 个的联邦、州、地方机构组成。在一次由基础设施部门负责的信息系统脆弱性调查中，来自其中 1 500 多个的机构的响应表明，这些组织已经越来越依靠信息与通信系统来执行其关键任务。这些系统面临的威胁在不断增长。这些 ELES 部门还依赖其他的关键基础设施，如能源和电信基础设施，而它们也容易遭到网络 and 物理破坏。

ELES 部门的关键基础设施保护计划展现了该部门为了确保其能够连续性地实施关键性应急执法职能而做出的初步战略。该计划代表了国家基础设施保护中心（NIPC），受命的 ELES 部门领导机构、ELES 论坛、来自于州和地方以及联邦非 FBI 机构的资深执法官员的联合努力。设立 ELES 论坛的目的是支持 ELES 计划的制定，使该论坛成为国家级应急执法事项的积极提倡者，并实现 ELES 界之间的联系。

该计划展现了 ELES 部门用来确定其最关键的资产、评估其脆弱性、制定修补和减缓计划的框架。它还提供了关于 NIPC 的威胁警报及通告系统的有关信息，以及各类基础设施和与信息安全相关的培训项目的信息。其伴随文档《州和地方政府执法机构指南》可以使 ELES 部门内的机构用来实施该计划中建议的活动。

这个指南可以作为 ELES 部门的基础性的基础设施保护教育和意识培养项目的文档。每个执法机构都有其运行的独立性，都要为其自己的基础设施保护做出响应。因此，任何部门级项目的成功都要依赖于每个机构去自愿地实施其计划中建议的各项活动。在国家级，ELES 部门领导层将在跨部门的规划和活动实施中一如既往地担任 ELES 部门的代表。

工作安排

第 3 级：关键部门——州和地方政府

建 议

政府与非政府实体可采取的用于增进网络安全的具体行动

R3-10 州和地方政府应当考虑为其下属各机构建立 IT 安全项目，包括意识培养、审计、和标准。州、地方和城市协会应考虑提供相关的援助、资料以及示范项目。

R3-11	州和地方政府应当考虑参与业已建立信息共享和分析中心（ISAC）。
R3-12	州和地方政府应当考虑扩展其面向执法官员的计算机犯罪培训项目，这些官员包括法官、检察官以及警察。联邦政府可以提供有关援助，对培训项目提供协调，并考虑在必要时提供资金方面的帮助。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	
行 动	
现有的网络安全工作	
P3-09	州首席信息安全官国家协会：www.nascio.org。NASCIO 发布了一份名为《公共-私营信息安全：对公共部门 CIO 活动的号召》的文献。
P3-10	国家州长协会：www.nga.org
P3-11	国家城市同盟：www.nic.org/nic_org/site
讨 论	
需要进一步分析、争议和讨论的重点问题	
D3-4	联邦、州、地方政府怎样才能增强对网络空间安全的协调和危机管理？
D3-5	在建立州间的信息共享和分析中心时，州政府可能会面临哪些特殊的法律或政策问题？

第三级之高等教育

美国的各个高等教育机构（IHE）——大学、四年制学院、社区学院已经制定了其有关目标，以采纳并实施某一特定级别的信息系统和网络安全项目，从而保护敏感信息并阻止系统被用作攻击其他系统的跳板。为此，各 IHE 确立了如下的行动框架：

- 在高等教育中，使 IT 安全成为优先课程。
- 更新安全策略，改善对现有的安全工具的使用。
- 提高未来的研究和教育网络的安全性。
- 改善高等教育、工业界、政府之间的合作。
- 把高等教育中的相关工作纳入国家的基础设施保护工作之中。

问题和挑战

最近的经验显示，很多不安全的计算机系统可以追溯到高等教育的校园网络，这些网络往往已经被黑客各个攻击后成为发起拒绝服务攻击或威胁 Internet 上其他不相干系统的平台。这些攻击威胁的不仅仅是目标系统，而且还有系统的业主以及期望使用系统上的服务的用户。

IHE 容易遭到这样的攻击，原因来自于如下两方面：（1）它们拥有巨大的计算能力；（2）它们允许对这些资源的相对开放的访问。IHE 拥有的计算能力很大，覆盖了 3 000 多所学校，很多院校拥有研究性计算设备以及巨大的中央计算设备。研究和教育机构占据了约 15% 的 Internet 域名。就这个规模而论，敌人渗透和“劫持”IHE 系统的目的，是可以借此发起对第三方系统的网络空间攻击（即“僵尸”现象）。它们无意中置其他基础设施部门于危险之中。

IHE 还拥有大量私有或保密的学生和员工信息。这些敏感信息（如疾病信息或医疗记录、学生信息、人事档案、敏感的研究信息）都放在大学的系统数据库中。于是，IHE 必须考虑更为广泛的网络空间的安全影响。

虽然 IHE 必须保护信息的隐秘性，阻止对其系统的恶意使用，但它们还必须提供一个供学生学习、供研究工作有效进行的环境。这两个需求并不是天生要发生冲突的，但 IHE 在制定其网络空间战略时必须同时考虑这两方面的需求。

战略讨论

总的来说，高等教育界已经在行动上做了一些工作，以组织其成员来增强美国校园的网络安全，并协调它们的行动。最值得称道的是，通过 EDUCAUSE，高等教育社会已经开始了对国家战略制定一事的

关注，包括高等教育的最高级领导，如美国教育委员会以及高等教育 IT 联盟。尤其是经过这些努力，一些上层大学的校长们已经采纳了五点行动框架，承诺要优先考虑 IT 安全，并要采纳那些对于实现更高的系统安全所必需的策略和措施。

美国的学员和大学还采纳了未来行动的工作安排表，以对付 IT 安全和信息保障的挑战。比如，除了国家科学基金会（NSF）外，EDUCAUSE 正在组织四个工作组。

第一个工作组将把高等教育界的领导们组织到一起，建立能够支持高等教育任务的安全战略原则。大学中研究界的代表们还将聚在一起，确定涉及教员和学生科研活动安全的有关问题、事项、和解决方案。

计算机和网络安全任务组

2000 年 7 月，EDUCAUSE 和 Internet2 建立了计算机和网络安全任务组 ([www.educause.edu/security](http://www.educause.edu/security))。高等教育界表示，该任务组的一个工作便是：扮演积极的角色，来发掘脆弱性以及导致脆弱性存在的系统缺陷；在校园中开发并实施安全解决方案。借这一行动，任务组希望能大大减少高等教育系统面临的直接威胁以及其他方面存在的非直接威胁。

在与兄弟协会以及著名专家的合作中，任务组针对高等教育中的安全问题制定了短期行动和中长期计划。其建议如下。

- 短期：所有的校园网和技术负责人应当采纳 SANS 学会提供的建议和方法来检查并纠正其网络上的 10 个最主要的安全漏洞。（10 个最主要的安全漏洞及相关资料可见 <http://www.sans.org/topten.htm>。——译者注）
- 中期：任务组将制定并公示改进后的有关流程和策略，来寻找、纠正、预防校园网上的安全缺陷，同时将制定并公示用来衡量和比较安全进展的有关手段。
- 长期：研究有助于以安全的方式实现新的服务，并能够系统地修补当前某些安全问题的下一代安全课题（如 Internet2 PKI 实验室 Internet2 高等教育 PKI 联合计划）。

工作安排	
第 3 级：关键部门——高等教育	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R3-13	每个学院和大学都应考虑建立在任何时候均可以联系到的联络点，当学校的 IT 系统被发现正在发起拒绝服务攻击时，能够让 ISP 和执法官员与学校保持联络。
R3-14	学校和大学应当考虑建立：（1）一个或多个信息共享和分析中心（ISAC），用以对付网络空间攻击和脆弱性；（2）示范性的指南，授予首席信息官（CIO）处理网络空间安全的权力；（3）一套或多套 IT 安全最佳实践措施文档；（4）示范性的用户意识培养项目和资料。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	

续表

行 动	
现有的网络安全工作	
P3-12	由 EDUCAUSE 和 Internet2 建立的计算机和网络安全任务组 <a href="http://www.educause.edu/security">www.educause.edu/security</a> 。
P3-13	国家科学基金会的 EDUCAUSE 系列工作组。
P3-14	EDUCAUSE 面向高等教育界领导和有关协会的推广和意识培养项目
讨 论	
需要进一步分析、争议和讨论的重点问题	
D3-6	为各高等教育机构（IHE）、学术机构、国家采纳一套示范性的授权中心的好处有哪些？（一个该类授权的例子可见 <a href="http://www.indiana.edu">www.indiana.edu</a> 。）
D3-7	是否应考虑把州和地方政府向 IHE 划拨的基金与其对某些安全基准的相符性联系起来？
D3-8	是否应建立高等教育界的信息共享和分析中心（ISAC）？如果需要，那么该如何建立？可以采取其他方法来改善在各级 IHE 间实现信息共享的方法吗？
D3-9	IHE 应当采纳国家标准与技术研究院（NIST）的“IT 安全保障框架”作为其信息系统安全一致性的标准吗？

### 第三级之私营部门

私营部门在保护网络空间安全方面扮演着中心角色，这是因为私营部门拥有并操作着非常多的国家基础设施，也因为这些基础设施所依赖的网络空间系统。某些关键基础设施部门已经花费了很大的努力来协调基础设施保护计划的制定。在这些过程中，私营部门确定出自己的战略目标，以保护由其拥有并运行的关键信息基础设施。这些计划对于美国政府面临的安全挑战的规模、范围、特征提供了无以估价的深入观察。

私营部门的计划对不同工业部门面临的挑战进行了具体的综述，并提供了它们为对付这些挑战而正在采取的措施。而且，工业界制定安全计划的活动还推动了网络空间安全的前进，因为它们建立的是一种行动步骤，私营部门可以在这些步骤中确定它们需要解决的安全问题；制定安全计划的活动还方便了基础设施保护事项的优先级的排序，在公共-私营合作联盟中，这种优先级的确定是必要的。

### 问题和挑战

网络空间的安全是一项共同承担的责任。没有一个工业部门可以完全对其安全负责，没有一个政府实体可以独自保护网络空间安全。应布什政府的要求，美国的关键基础设施部门已经采取了前所未有的努力来针对网

关键基础设施部门	部门协调机构/成员机构
银行与金融	美国银行协会、安全工业协会、BITS、金融服务信息共享和分析中心委员会、美国独立社区银行协会
电力	北美电力可靠性委员会
石油和天然气	国家石油委员会
供水	受到美国水工业协会支持的大城市供水机构协会、供水企业国家协会、AWWA 研究基金会
运输（铁路）	美国铁路协会
信息与通信	蜂窝电信和 Internet 协会、美国信息技术协会、电信工业协会、美国电信协会
化学	化学部门网络空间安全信息共享论坛
这些基础设施部门的计划可见 <a href="http://www.pcis.org">www.pcis.org</a> 或 <a href="http://www.ciao.org">www.ciao.org</a>	

络空间和物理安全的保护而制定关键基础设施保护计划。各类部门的战略中分别描述了各工业部门为保障其关键的基础设施运行不会受到网络空间攻击或物理事件的破坏或危害而正在采取的行动。私营部门的计划旨在加强基础设施安全并对联邦政府的安全规划工作提供补充。所有这些计划都为一个真正的国家战略奠定了基础。

关键基础设施合作组织（PCIS）是一个由关键基础设施公司组成的非营利机构。它的成立就是为了解决基础设施保护涉及的复杂问题。PCIS 由 8 大基础设施部门中的 60 多家会员公司和 13 家政府机构组成，这是一种联合性的努力。

PCIS 的任务是协调跨部门间的基础设施保护活动，为公共-私营部门的安全工作提供补充，以便当经济和国家安全出现风险时，能够保障关键基础设施服务的可靠提供。

PCIS 和 CIAO 已经审查了表中所列的各基础设施部门安全保护计划，并对各部门中的公共事项和所关心的问题作了摘要。PCIS/CIAO 的分析报告可以在 PCIS 网站上得到（[www.pcis.org](http://www.pcis.org)）。

拥有和操作关键基础设施的各公司们面临着六项共同的挑战。为加强基础设施的保护工作，这些挑战必须得到解决。它们包括很广泛的议题，如基础设施互依赖性、研究和开发、教育和人员培养、信息共享和分析、公共政策和法律挑战、国际事项。

#### （1）基础设施互依赖性

在过去的 10 年间，美国的基础设施已经把 IT 和网络空间集成到了其运行的所有方面。

与 IT 的迅速融合带来了巨大的效率，促进了革新，增强了服务的可靠性。但与专有系统相分离的不同基础设施之间，一旦需要相互集成，这种集成就会产生很多复杂的互依赖性问题。在很多情况下，这种互依赖性还没有得到充分的理解。

工业界正在与政府合作，努力理解这种存在于各基础设施部门与政府间的复杂的互联性问题。特别地，人们开始关心从一个基础设施部门到另一个基础设施部门的级联问题。有必要开发相关工具和方法来实施网络空间的风险建模，以消除掉脆弱性并发展合适的风险转移机制。保险界和再保险界已经开始实施很多努力去支持这些工作。（若需更多关于保险界的有关信息，请参阅 [www.pcis.org](http://www.pcis.org) 或 [www.ciao.org](http://www.ciao.org)。）

#### （2）研究和开发

网络空间的安全研究和开发（R&D）是私营部门必须解决的另外一项挑战。在私营部门中，每个工业领域都有其独特而具体的 R&D 挑战，这些挑战已经得到了每个工业领域的解释，并且可以在它们各自的计划中找到。还有某些 R&D 挑战的交叉性更强一些，并且包含了诸如脆弱性评估方针和应急规划中的最佳实践措施等事项。

#### （3）教育和人员培养

对基础设施安全的改善要以人为基础。高级管理、技术人员、雇员群体都扮演着重要的角色。当高级管理层开发了旨在提高网络空间安全风险意识的项目时，它们随后就可以设置管理策略来促进基础设施的安全性。然而，为了实施这些管理策略，基础设施还需要去雇用经过良好培训的技术人员。而合适的技术人员的获得要大大依赖于教育和培训项目。最后，一个基础设施部门的安全将依赖于雇员能够遵循机构的计算机安全策略的综合水平。在促进所有基础设施的网络空间安全方面，上述三项因素扮演着决定性的角色。

#### （4）信息共享和分析

工业界和政府正在联合促进信息的共享和分析。当前，一些独立的关键基础设施部门正建



立能够在其作用范畴之内实现安全信息共享的机制。而且，还有几个基础设施部门正不断开发进一步的手段，使它们能借此超越其自身的工业领域，在跨部门间以及与政府之间共享涉及威胁、脆弱性、对策和最佳实践措施的信息。

#### （5）公共政策和法律挑战

在各自的计划制定中，每个部门都确定了很多公共政策，在某些情况下，还指出了有可能阻碍其基础设施保护和网络空间安全的一些法律问题。在分析报告中，PCIS 提供了对私营部门的这一问题更加详细的讨论。

#### （6）国际事项

网络空间安全是一项国际性的挑战，它不是由任何物理的国家边界所包围的。多个部门的操作都横跨了国际边界。因此，全球基础设施领域正在努力保护它们的公共信息系统的可用性、完整性和可靠性。

### 战略讨论

#### （1）培育更加有力的公共-私营合作联盟

信息共享和分析中心（ISAC）在国土安全和网络空间安全中扮演着越来越关键的角色。ISAC 一般都是一种由工业界领导的机制，用于收集、分析、过滤、传播同特定部门相关的安全信息。由各基础设施部门设立的 ISAC 是为了满足其响应需求，并由 ISAC 的成员提供基金支持。（电信界的 ISAC 位于国家通信系统局，由政府资助。）各 ISAC 通过国家基础设施保护中心（NIPC）与联邦政府密切合作，互相交换关于威胁和脆弱性的信息，并通过 CIAO 来实施协调和规划工作。总统提议成立的国土安全部将整合 NIPC、CIAO 以及联邦其他网络空间中心，以使信息共享机制流畅化，并增强基础设施的分析能力。

建立信息共享和分析中心需要部门内的大量合作，还需要建立一个清晰的业务模型。虽然各 ISAC 均不相同，但不论是新建还是已建的 ISAC 都必须克服很多挑战，包括改善基础设施业务在 ISAC 中的参与情况；增强威胁信息的时效性和效率；克服信息共享面临的困难。一些基础设施部门已经或正在规划建立它们自己的与其具体的工业领域相关的 ISAC。

在很多部门间，ISAC 正在发展和成熟，包括电信、金融服务、信息技术、供水、运输、电能、石油和天然气、化学、食品、州政府以及其他领域。它们吸收了各个领域内的技术专家，能够促进安全事件的管理和解决。

为了响应未来的挑战，ISAC 可能需要链接到政府的预警和分析中心。故当前某些努力工作还在进行，期望考查 ISAC 进行互联以及与关键性的政府中心相链接时的优势。这可能会促进关键基础设施信息的及时流动，并可以加强危机管理工作。

当 ISAC 成熟时，国家对网络空间事件和攻击的响应和管理能力也将会变得成熟。除此之外，联邦政府和 ISAC 可能会研究基础设施的分析功能所面临的挑战，并圈定一批有可能用来对脆弱性、攻击行为以及修补活动进行可视化和理解的有关方法和工具。

若有必要，联邦政府有可能会通过 ISAC 来提供技术援助，以帮助制定关键基础设施的应急和危机管理计划。除此之外，联邦、州、地方政府也可以探讨有关的途径，在发生重大破坏事件以至于对该事件的处理已经超出了一个或几个公司的能力范畴之外时，对响应和恢复活动进行协调。

工作安排	
第 3 级：关键部门——私营部门	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R3-15	每个基础设施部门都应考虑建立一个信息共享和分析中心（ISAC），并与其他 ISAC 保持协作。联邦政府将考查根据需要把各个 ISAC 与适当的网络安全预警和分析中心相联的情况，并将促进在必要时对关键基础设施保护信息的提供。
R3-16	每个关键基础设施部门都应考虑针对技术缺陷以及研发缺陷实施分析，与科技政策办公室（OSTP）的工作相协作，为联邦政府网络空间安全研究排定优先级，以解决这些技术和研发中存在的缺陷。各关键基础设施部门和 OSTP 应在这些研究活动的实施中保持协调。
R3-17	每个关键基础设施部门都应考虑制定网络空间安全的最佳实践措施，并在必要时提供安全的 IT 产品和服务采购的方针指南。
R3-18	每个关键基础设施部门都应考虑部门内的彼此合作，以实施面向具体部门的信息安全意识培养运动。
R3-19	每个关键基础设施部门都应考虑建立网络空间安全应急响应的互助计划。司法部和联邦贸易委员会将与各基础设施部门共同工作，以解决互助合作中出现的任何壁垒。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体特定的、不断变化的环境	
行 动	
现有的网络安全工作	
P3-15	关键基础设施安全合作组织：www.pcis.org

8. 第 4 级：国家的优先任务

在实施国家的优先任务时，总的战略目标是建立网络空间安全的基石。包括如下三个重要的网络空间安全基石：

- 保护共享系统的安全；
- 培育一个强有力的经济和社会框架；
- 制定国家计划和政策；

为建立这些基石，我们将需要实施一系列清晰定义的工作。这些工作都要置于国家级的层面上，并将为我们的国民在本战略中的各个级别上采取行动时提供支持。比如，研究如何加强当前的基础设施安全性或研究发明新的信息保护方法，这会使从家庭、工业界以及政府内的所有人士受益。本节概要介绍了国家在 17 个网络空间安全领域正在实施的工作。

网络空间安全所依赖的关键基石	为奠定这些基石所需的工作
保护共享系统的安全	保护 Internet 机制
	监督控制和数据采集（SCADA）系统研究
	高度安全和可信的计算
	保护新兴系统的安全
	脆弱性矫正

续表

网络空间安全所依赖的关键基石	为奠定这些基石所需的工作
培育一个强有力的经济和社会框架	意识培养 培训和教育 认证 信息共享 网络空间犯罪 市场推动力 隐私
制定国家计划和政策	分析和预警 运营连续性、重建和恢复 国家安全 互依赖性和物理安全

### 保护共享系统的安全

在网络空间的基本元素更加安全和更加可靠后，各级用户将从中受益。政府最好能够找到可以使计算设备，尤其是操作系统更加安全的途径，并能够保护互联网络的安全性，确保新添加的组件和设备的充分安全。通用系统中的一项安全性改进，相当于单个用户的几百万项安全性改进。当发生脆弱性时，必须有有效的脆弱性矫正手段。保护共享系统的战略目标是通过保护所有各级用户的通用系统，大大增强个体的安全。

#### （1）保护 Internet 机制

Internet 最初开发时，其创建者不会设想经济、国家安全以及 Internet 最终需要具有的应急战备目的。他们没有意识到 Internet 随时间而发展的速度和规模。于是，在 Internet 最初建造时，类似于安全性的很多在现在看来非常重要的特性，却没有成为 Internet 基础的一部分。

Internet 有冗余性，安全可以不断地加入。但是，安全从来就没有被融合成 Internet 的基础特性，而且在安全的实现上也还存在着诸多缺陷。除此之外，Internet 用来通信的方法和规则以及支撑信息传输的设备均不是为支持日益膨胀的信息在 Internet 上流动而设计的。

Internet 安全机制的开发和实施是其业主、操作者以及用户的共同责任，单个实体或组织无法完成这项工作。而且，这其中还需要一个合作联盟。由私营工业正在领导的很多工作是为了使 Internet 的功能能够以安全的方式发展。必要时，联邦政府会持久地对这些工作提供支持。

此中的战略目标是促进安全和稳健的 Internet 机制的开发，使 Internet 能够支持国家当前以及未来的需求。需做的工作包括：

- 改善关键 Internet 协议的安全性和抵抗力；
- 提高路由安全；
- 采纳最好的安全标准、实施方法及准则，即“良好的实施规范”；
- 建立公共-私营合作联盟，探求和解决基础性的 Internet 技术需求。

#### （2）监督控制和数据采集（SCADA）系统

过去 20 年来，美国很多工业部门的设备控制和监督方式已经发生了根本性的改变。以前，系统由工人们以人工方式控制，这需要工人在物理上位于设备端；而如今，很多这样的系统已

经通过网络远程控制，在一些案例中，Internet 成为了信息流通的必要手段。

这些公司对其控制系统的保护能力由于两个原因而受到限制：首先，很多公司不愿意对安全投入资金；其次，在技术上还存在着一些缺陷。SCADA 系统通常不大，且是独立的自控制系统，其能量输入有限，而且运行于实时模式。这意味着安全特性有可能削弱 SCADA 系统的性能，或还需要其他的操作能源，因此在 SCADA 系统上实现安全性确实有难度。

我们的战略目标是使 DCS（数字控制系统）和 SCADA 系统的用户有能力去保护他们的网络空间，防止其系统被用来破坏国家的关键基础设施。为实现该目标，需要完成下列事项：

- 提高工业提供商和用户对 SCADA 系统中的脆弱性的意识，并使他们意识到这些脆弱性被利用后所带来的后果。
- 制定和部署如下专题的培训与认证项目：数据安全基础、面向 DCS/SCADA 的安全、软件安全、硬件安全等。
- 推动标准化、安全策略的制定等工作，加强这些标准和策略的实施手段。
- 提供测试床环境，用以研究安全问题和所提交的安全解决方案。
- 在如下领域展开研发：超低延迟链路加密机/鉴别器、密钥管理、网络状态监测。
- 确立政府/工业界合作联盟，确定与 DCS/SCADA 有关的最关键的场所，并为这些场所制定安全计划，以提高其网络空间的安全。

### （3）研究

当国家对网络空间的依赖不断增强时，联邦在下一代网络空间安全技术方面的投资一定不能落后于不断增多的脆弱性数目。为了确保研发过程能与不断发展的技术环境相对应，重要的是保持一种灵活性。在财政投入与寻找和修补脆弱性这两个问题中，应求得适当的平衡，这便要求在未来投入更多的资金。国家会对网络空间安全研究活动的优先级进行排序，并为这些研究活动的前进而提供必要的资源。

新一代的安全技术将会使 Internet “现代化”，使其适合于快速增长的通信流量和不断扩张的电子商务，并能够满足下一代网络广泛部署时出现的一些高级应用。因此，国家级研究工作必须优先考虑对网络空间安全的支持，使网络空间成为一个 21 世纪的安全、高速的知识交换和通信基础设施。

这项工作需要一些非常重要的研究内容。比如，必须对数字控制系统开发出加密和鉴别功能。在所有的基础设施部门以及基金源中，国家必须优先考虑其网络空间安全方面的研究。

国家级网络空间安全研发的战略目标是协调各项技术的发展，以对抗威胁、较少脆弱性，并面向未来培育建设起一个有抵抗性的、安全的网络空间。这将通过如下工作来实现：

- 制定年度的网络空间安全研发规划，分别满足短期、中期以及长期的目标。
- 在网络空间安全领域领导一个充满活力的联邦研发项目，以求快速标明、发展并促进威胁和脆弱性对抗技术和工具的落实。
- 在私营部门、学术界、国际社会之间培育起一个密切的合作联盟，以确保每项关键的技术都得到考虑，并使新的安全技术得到迅速采纳。
- 确保联邦政府的 2004 财年网络空间安全预算与国家级的研发重点相一致。

### （4）高度安全和可信的计算

在未来的某一天，我们会离不开对计算机、Internet 以及其他任何网络空间系统的操作，就像我们无法不去开灯或打开水龙头一样。它们将会成为一种必然的东西，融入我们的生活。

然而现在，计算机或系统长时间遭到破坏或无法使用的情况是很普遍的。数据常常丢失，要么就是费尽九牛二虎之力才能接收到。系统常因为其组件受损而超载或出错。

我们的战略目标是确保未来的网络空间基础设施组件的内在安全和可靠。这要通过下列工作来实现：

- 进一步研发高度安全可靠的系统。
- 建立软件开发过程方法以及质量保证测试机制，以制造出安全可靠的产品。
- 发展在软件中检查恶意代码的功能。
- 重新改革联邦的采购标准，在其中坚决要求安全性，并严格执行这些标准。

#### （5）保护新兴系统的安全

新兴技术在发展时也可能同时引入新的脆弱性。无线局域网便是一个实例。虽然在系统的开发中人们已经对此作了特别注意，但在操作环境下实施时，这些系统仍然表现出了某些弱点。今天，一个人驾车绕城一圈就可以找到很多无线局域网络去访问，不论这些网络归谁所有。只要入侵者愿意，他就可能从这些新兴系统中偷窃信息，或发起对系统的攻击。加入某些安全机制（如口令访问要求、地址过滤、加密、使用 VPN）后，它们被攻击的可能性就会大大减小。然而，司空见惯的是，由于这些安全机制涉及的复杂性、成本或时间，它们常常未得到实现。即使当厂商安装了安全机制后，也有可能因为口令遭到破坏而发生入侵事件。因此当新系统进入市场并广泛普及后，必须努力确保其充分的安全性。

新兴技术可能会产生难以预见的安全后果。光计算、智能代理以及长期研究领域中的纳米技术和量子计算等，均有可能对网络空间带来变革并影响其安全。我们的国家必须站在领导位置上去探究这些技术及它们对安全的影响。

我们的战略目标是发现由新兴技术而导致的网络空间的脆弱性，并思考如何去消除、降低或者管理由这些脆弱性所带来的潜在风险。该目标的实现要依靠以下努力：

- 改善新兴技术的安全性。比如无线局域网（WLAN）中，其安全性的改善将通过下列手段实现：增强人们的安全意识及 WLAN 的易用性；发展新一代的安全无线技术；研究 ad hoc 网络和格计算中的安全问题。
- 不断审查新兴技术的安全性。

#### （6）脆弱性矫正

新的脆弱性每天都在出现，软件使用中暴露出的缺陷可以被犯罪分子利用来发起恶意行为。当前，每年报告的脆弱性数目大约有 3 500 个，而这些脆弱性的修补往往是生产商以补丁的形式并通过补丁的分发来完成的。

很多已知的缺陷却长时间得不到改正。比如，相当多已报告的网络空间攻击事件的罪魁祸首就是我们前面说过的十大漏洞。导致这种现象的原因是多方面的。很多系统管理员可能缺乏足够培训，或者没有时间去查看是否每个补丁都已安装到系统上。待安装补丁的系统有可能会影响到其复杂的互联系统集，要确信补丁可以安装之前，必须花费较长的时间去测试。如果系统很关键，那么就很可能难以将其关闭来安装补丁。

我们的战略目标是：在近期，通过改善有关工具和方法，能够极大地提高脆弱性修补时的速度、覆盖范围、有效性；在远期，要从源头上减少脆弱性的存在。该目标可通过如下工作来实现：

- 制定脆弱性修补的最佳操作方法，并推动各公司和机构对最佳操作方法的接受。

- 创建一个中立的信息交流机关，以更快地判断脆弱性补丁对通用应用程序造成的影响，包括可能的测试结果。
- 研究并鼓励对补丁影响信息的正确披露，从而加速补丁的有效实施。
- 开发并实现改良的代码技术和质量保证标准，以减少脆弱性的数目。
- 使更多软件在交付时能达到一个安全的初始配置状态。

### 培育一个强有力的经济和社会框架

为加强并维护网络空间系统的安全，系统所存在的这个社会的法律和准则必须能够以强有力的方式来对其安全起到强化作用。这些机制包括通过法律手段来对付网络空间犯罪，通过法规和 Related 组织来促进信息的共享，通过学习机构来培训和教育安全人员。应坚持某些基本的原则，如要认识到市场的角色以及隐私保护的重要性和核心性，这也有助于进一步实现社会化安全机制。国家战略的目的便是培育起一个经济和社会框架，以一种自然平滑且稳固的途径来使用安全并同时加强这种安全性。

#### (1) 意识培养

很多情况下，人们不是没有网络空间安全问题的解决方案，而是需要这些方案的人们不知道它们的存在，或者不知道如何或到哪里去找到这些方案。而在另一些情况中，人们甚至没有意识到网络安全的需求。比如，一个小型商业可能就不会想到其 Web 服务器使用的是任何人都可以用来登录系统的默认口令。为了使用户和操作员敏感到其安全需求，教育和推广活动便扮演了重要的角色。在本战略讨论的几乎所有问题中，这些教育和推广活动都可以成为解决方案的一部分，从工业界中数字控制系统的保护，到家庭中电缆 Modem 的安全。

我们在此中的战略目标是使所有人都懂得网络空间的安全问题和解决方案，从而激励大家行动起来去保护我们的网络空间安全。这要通过下列工作实现：

- 以现有的工作为基础，并进一步扩展现有的工作，引导机构的关键决策者（如 CEO 及董事会成员）在其业务中考虑如何去保护机构的信息系统安全。
- 通过各项有关计划的实施来使州和地方政府的关键决策者（如州长、州议员、市长、县行政官/县监事会等）支持信息系统安全方面的投资，并使他们能够采纳可行的安全管理政策和措施。
- 向广泛的用户、学生、儿童、小型商业机构灌输基础的网络空间防护/安全教育。
- 通过与当地机构、中小学的交流与合作，使网络空间的安全问题为更多人所知，并促进大家对可参考的安全资源的了解。

#### (2) 培训和教育

为实现并维护网络空间安全，我们国家需要很多受过良好培训的、富有才华和创新精神的人才。虽然，随着 Internet 的扩张以及计算机、网络和其他网络空间设备的普及，对这些人才的需求已经迅速增长，但培训方面的投入却还未跟上。各大学中，工程专业的毕业生越来越不够，他们的大部分资源已经被其他学科占用了，如生物学或生命科学。虽然如今的计算机网络已经广泛普及，且它们的安全问题也已经广为人知，但很少有小学或中学学生能够得到网络空间安全课程或课件的教育。美国要想在网络空间经济中领导这个世界，这一趋势就必须制止。

我们的战略目标包括：（1）培养并保持众多受过良好培训的、技术高超的、我们国家自己的 IT 安全专家，满足日益增长的国家需求；（2）在大众中培育起基本的网络空间安全技能以

及网络空间的道德规范。这些目标要靠如下工作来实现：

- 面向各级教育，推行由州和地方政府及私营实体制定的各项指南，内容涉及网络空间的意识培养和知识学习、培训以及教育，包括针对网络空间中道德行为的教育。
- 对当前现有的教育项目加以扩展，使更多四年制学院和大学能开设高质量的 IT 安全项目，通过非学位的教育项目、职业学校、初级学院、技术学会等途径增加 IT 安全技能的培训机会。
- 创建一个国家级的网络空间学会，把联邦政府的网络空间安全和计算机取证学方面的培训项目联合起来。
- 在联邦政府和私营工业的每个部门中，都建立清晰定义的 IT 安全职务和专业。
- 确保在工作中能得到不断的教育和高级培训，以培养高超的技能和创新能力。

### （3）认证

与教育和培训相关联的需求便是合格人员的认证。认证可以为雇主和客户提供更多的关于待聘雇员或安全顾问的能力的有关信息。现在已经有了—些网络空间安全工程师的认证项目，然而，它们在各自的认证要求方面差别甚大。比如，某些认证项目强调的是广泛的知识面，并通过综合性的多项选择题来考查；而有的项目则考查一个人对某个具体的网络空间组件所具有的深层次的实践知识。还没有哪个认证项目能够对一个人的实践和学术能力提供适度的保障，无法同医师、法律、会计职业认证相比。

我们的战略目标是—为 IT 安全专家认证建立起—套在国家范围内得到认可的标准，以确保 IT 系统和网络的评估与维护能保持一致性和有效性。需要做的工作如下：

- 强化现有的认证项目，在必要时发展新的能力，创建能够与会计、法律、医师认证过程相比拟的 IT 安全专家的对等认证标准。认证的范围可包括高级水平的国家级标准考试、由专业机构主管的考试、服务于私营工业的 IT 顾问认证考试。
- 建立认可机构，负责检查各种认证项目是否满足了系统管理或相应职位上的最小标准集。
- 联邦政府在招聘某些级别的 IT 专家时，应对认证提出要求，并在—段时间以后，应对其当前所有雇员提出认证要求。

### （4）信息共享

国家必须能够以实时方式对网络空间的事故以及攻击加以检测和分析。有关这些事故或攻击事件的自愿式的信息共享将在网络空间安全中起到至关重要的作用。而—些实际存在或预料到的某些法律障碍可能会使某些公司畏葸不前，难以同联邦政府或在几个公司彼此间共享事件信息。首先，某些人担心共享的数据有可能是保密的或有知识产权问题，或者会使公司陷入窘境，一旦与政府间实现共享，则这些信息便可能会被公众看到。其次，—些人也担心，在工业界中，各公司之间的信息共享还会受限于利益竞争。最后，有时也仅仅是因为找不到有效的信息共享机制。

我们的战略目标是增强公共—私营实体以及私营部门实体间对网络空间安全信息的自愿式共享。为此，应完成如下工作：

- 强化现有的信息共享机制，以确保这些机制的充分性，使它们能够覆盖所有必要的信息源。
- 为关键信息的共享创造—个良好的法律和政治环境，消除人们对于共享信息的使用方

面的担心。

#### (5) 网络空间犯罪

一旦检测到安全事件，就必须解决。通过快速响应可以遏制住正在发生中的攻击，并减弱其最终可能造成的损失。我们国家现在有很多可确保对大规模事件发起快速响应的法律和机制。这种响应还包括为事件中受到影响的业主和用户分析并传递实用的信息。理想的是，这之后马上开展对入侵者的调查、逮捕和起诉。如果入侵行为是由某个国家发起的，则还可能还会涉及外交或军事行动。遗憾的是，常常有很多事件得不到报告，而且有时即使报告了入侵事件，当地机关也会因缺乏培训或经验缺陷而无法有效地做出响应。各州和地方政府内执法机关的水平也极为参差不齐。

我们的战略目标是预防、检测并大大减弱网络空间的攻击，以确保能够发现正在活动或试图进攻的攻击者，并随后由政府发起适当的响应，在出现网络空间犯罪时，还要迅速逮捕并对犯罪者施以必要的严厉惩处。这将通过下列工作实现：

- 改善联邦、州和地方政府内负责关键基础设施保护和网络空间安全事务的执法界内及他们同其他机构和私营部门之间的信息共享和调查工作的协调。
- 不断评估联邦判决准则对网络空间犯罪处罚的力度，确保每次网络空间犯罪都得到应有的惩罚。
- 增强联邦、州和地方执法机构的能力，努力为其提供足够的调查和取证资源，并向它们提供培训，方便其在关键基础设施事件中的调查取证工作及对事件的解决。
- 为网络空间犯罪和入侵事件中的受害者建立详细的数据。
- 参与国际合作，以获得合适的网络空间事件响应工具。

#### (6) 市场推动力

大部分网络空间都经历了私营及无序运行的历史和传统，是私营部门的投资和创新使得Internet，更普遍地说，是网络空间成为了当前这样至关重要且稳健的基础设施。而当网络空间成为了国家关键基础设施的一个重要组成部分时，我们对其安全、可靠和防护性的需求也显得势在必行。要满足这一需求，就需要网络空间中各业主和提供商增加进一步的投入并提供更多的资源。

确保投入到位的最好的办法就是让市场提出需求，而不是让政府去下命令。某些时候，政府可能会通过政策来鼓励私营部门的参与，比如在意识培养工作中宣传网络空间安全的重要性。此外，还可以通过推荐性标准和标准化活动来影响政府系统的投资和采购，也可诉诸公共-私营合作联盟。应为这些市场推动力的有效发挥而努力创造环境。在其中，不要去诉诸有关网络空间安全的法规条例，除非有凌驾一切的需求去保护美国人民的健康、安全和福利。

此中的战略目标是在促进和加强网络空间安全的过程中尽可能减小对市场的干预。该目标可通过如下工作实现：

- 充分利用机构管理层和工业界中标准制定者的工作，促进网络空间的安全。
- 与保险界合作，推动网络空间安全风险转移机制的实施。
- 建设更加清晰透明的安全储备，推广最佳实践措施，这有可能要通过自我管理机构来实现，如市场交换手段。
- 通过向私营部门的技术转化，开发创新性的网络空间安全产品和服务。



### （7）隐私和公民自由

国家战略必须与这个开放、民主的社会中的核心价值相一致。同样，美国人民希望政府和工业界能够尊重他们的隐私，防止隐私遭到滥用。这种对隐私的尊重正是我们国家的力量之源，因此，确保网络空间中的数据的完整性、可靠性、可用性、保密性的最重要的原因之一便是当美国人民使用网络，或者当他们的个人信息保存于网络时，去保护美国人民的隐私和公民自由。为此，我们的国家战略中体现了隐私原则，不只是在某一章内，而是通篇之中。我们将坚定不移地致力于寻求既能增强安全性、也能保护隐私和公民自由的解决方案。

我们的战略目标是在实现网络空间的安全性的同时，不致损害个人的隐私和公民自由。该目标将通过下述步骤来完成：

- 继续履行政府的承诺，严格实施已有的隐私和公民自由保护法律。
- 经常同隐私提倡者、工业界专家以及公众相协商，确保在国家战略的实施中能尽最大可能地吸收国民对隐私问题的看法，尽可能地考虑到隐私问题，从而在加强网络和主机安全的同时也能对隐私提供保护。
- 扩大当前的年度 GISRA 审计项目的范围，审查每个联邦机构中的隐私保护事项。
- 鼓励工业界在制定规划以及生产产品时以自愿的方式加入必要的隐私保护。
- 确保联邦政府通过具体实例起到领导作用，在各机构中实施强隐私政策和措施。
- 就隐私问题和相关政策向终端用户实施教育，并鼓励他们在隐私事项中能够做出有意识的选择。

### 制定国家计划和政策

这是国家级事项的第三大类问题，它涉及国家计划及政策的制定，以对付关键基础设施遭到的有组织的攻击，防止由于攻击或自然事故而导致的基础设施瘫痪。这种瘫痪的后果必须得到充分的研究，因为关键基础设施是高度互联的，其瘫痪后果可能很复杂，且难以建模。一旦我们充分理解了这种后果，国家就必须制定相应计划来有效且高效地响应这种大规模的安全事件。下文讨论了国家政策和计划中四方面的重要问题。

#### （1）分析和预警

我们国家对网络空间事故或攻击进行响应的能力要首先依赖于对这些事故的早期检测能力。现在，政府和私营部门的很多机构，均在收集 Internet、互联网络及信息系统上出现的各种事件和脆弱性信息。还有的机构能够把这些信息传播给需要它们的人，以帮助其减弱可能的负面后果。很多工业部门已经建设了信息共享和分析中心（ISAC），能够向该部门中的所有公司发布早期的事件信息。各 ISAC 和政府之间还可以通过双向的途径共享信息。

虽然在检测和信息传播方面，我们已经取得了一些进步，但缺陷依然存在。对 Internet 服务提供商（ISP）以及作为一个整体的国家来说，还没有一个用来发布预警信息的专一的信息收集和发布中心，也没有一个得到了清晰定义的联合事件响应流程或团队。预分析功能也十分欠缺，且常受到信息匮乏的困扰。而且，很多事件信息来自于敏感机关，它们常与国家安全联系在一起。

我们的战略目标是：在事件的早期实施检测，高效地响应这些事件，并尽最大可能提前预知它们。该目标要通过下列工作来实现：

- 对建立国家网络运行中心一事进行研究。

- 改善政府的数据分析功能，包括提高对各机构的数据的使用率。
- 鼓励公共-私营实体间不断扩展数据共享和分析功能。
- 加速事件响应功能的改善和扩展。

#### (2) 运营连续性、重建和恢复

对网络空间重大事故或破坏进行响应的综合性公共-私营计划将会使我们国家从中获益。很多机构已经制定了在大型网络空间事故或灾难中恢复其网络功能的计划。然而，我们还缺乏相应的机制来统一协调公共及私营部门中的这类计划。

我们的战略目标是提供一个国家级的运营连续性及重建和恢复计划，当一个或多个部门的 IT 系统发生大规模事故时，能够确保服务的连续性，或设法将其恢复和重建。为此，公共-私营界需要完成下列工作：

- 协调并不断更新网络空间安全应急计划的制定，包括 Internet 功能的恢复计划。
- 确定在网络空间安全应急计划或 Internet 恢复计划启动时所要求的门限值。
- 经常性地演习应急或恢复计划。

#### (3) 国家安全

我们国家面临的敌人还包括外国政府和恐怖分子集团，它们能在国家安全的层次上发动网络攻击。在和平年代，美国的敌人可能会对我们的政府、大学的研究中心以及私营公司实施间谍活动；在对峙时期，他们将会通过研究美国的信息系统、确定重点攻击目标、在关键基础设施中安装后门或其他手段来储备网络战能力；而在战争或危机时期，他们则可能通过攻击我们的关键基础设施和重点经济功能，或者通过削弱公众对信息系统的信心而威胁我国的政治领袖。他们还可能试图借由对国防部、情报界、其他政府机构或关键基础设施的系统的破坏来延缓美国的军事响应能力。

我们的战略目标是改善我们国家在网络空间中的安全状况，限制敌人对美国施压的能力，一旦发现威胁就将其迅速消除。国家安全委员会、国防部、司法部、情报界或其他联邦机构应当：

- 与州、地方政府和私营部门密切合作，提高国家整体的网络空间安全状况。
- 发展强有力的反情报能力，以对抗美国政府、商业和教育机关所遭到的网络空间情报搜集势力。
- 使国家能够迅速定位威胁性攻击或行为源，并能在攻击发生前便可将威胁加以抑制。
- 在执法机构、国家安全机构、国防机构之间，改善对重大攻击的事件响应协调过程的认识。
- 当美国的核心利益受到网络空间的攻击所威胁时，保留实时响应的权力。

当敌对国家、恐怖主义集团或其他对手通过网络空间攻击我们国家时，美国不会排除以法律起诉甚至信息战为手段进行响应。当美国的核心利益受到网络空间的攻击所威胁时，美国将保留实时响应的权力，就像对待任何其他类型的侵略一样。

#### (4) 互依赖性和物理安全

当一个基础设施遭到破坏时，其他基础设施也常常会受到影响。甚至网络空间中的破坏性事件也会影响到物理空间，反之亦然。一列火车在巴尔的摩隧道出轨后，芝加哥的 Internet 的速度也受到了影响；而由于墨西哥州的某次篝火晚会破坏了天然气管道，硅谷内与 IT 有关的产品纷纷止步不前；地球上空数百英里处的卫星失控后，受到影响的银行客户便无法再使用其 ATM。

网络空间同时也有很多物理形式的表现，比如通信和 Internet 网络就要靠建筑物和导线所支持。在设计和建造时，这些物理元素已经包含了冗余特性，可以避免单点故障。然而，运营商和服务提供商仍应彼此合作，共同分析其网络，增强网络的可靠性和冗余特性。FCC（联邦通信委员会）和 PCIPB（总统关键基础设施保护委员会）可以支持这些工作，并应负责查明在国家网络的加固过程中可能存在的任何政府阻碍，FCC 的工作由其下属的 NRIC（国家可靠性和互操作性会议）实施，而 PCIPB 的工作则通过 NSTAC（国家安全电信咨询委员会）实施。

我们的战略目标是减少某处基础设施的故障对其他基础设施可能带来的负面影响。

为实现该目标，政府和私营工业需要完成下列工作：

- 在关键基础设施业主、政府以及负责系统建模和解决方案开发的私营集团之间培育信息共享体制。
- 针对关键基础设施的互依赖性，发展一种强健的国家级建模功能。
- 在关键基础设施的业主和操作者之间，就基础设施在出现故障时产生的互依赖影响以及消除互依赖负面影响的步骤而提高大家的意识。

工作安排	
第 4 级：国家的优先任务	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R4-1	公共-私营合作联盟应当优化并促进边界网关协议、IP 协议、DNS 及其他协议对改良的安全特性的吸收。
R4-2	公共-私营合作联盟应当完善并促进对更安全的路由技术和管理技术的吸收，如带外管理。
R4-3	从第一级公司开始的 Internet 服务提供商或大型的接入提供商应当考虑采纳“优秀操作规则”来管理其涉及网络空间安全的行为，包括与其他公司之间开展的与安全事项有关的合作。
R4-4	公共-私营合作联盟应当确认并解决基础性的 Internet 技术需求，这其中有可能要利用已有的项目，也许还要为这些活动建立基金。
R4-5	公共-私营合作联盟应当制定最佳实践措施并发展新技术，以增强 DCS（数字控制系统）和 SCADA（监督控制和数据采集）系统在公共事业、制造业及其他网络中的安全性，此事应被置予极高的优先级。
R4-6	政府和工业界应该合作确定最为关键的 DCS/SCADA 相关场所，并为这些场所制定一个优先级已经得到排序的安全改善计划。DCS/SCADA 用户应考虑采纳能源部的文献《提高 SCADA 网络安全性的 21 个步骤》。
R4-7	PCIPB 的研发委员会应针对现有的推广机制、学术界和工业及政府界间的研发活动的确定和协调而实施综合性的审查和缺陷分析。在 2003 年 2 月，委员会应完成上述工作，并向 PCIPB 提交其建议书，对上述机制的实现、扩展及建设提出建议。
R4-8	PCIPB 应负责在每年度与科技政策办公室（OSTP）主任和 PCIPB 下属的研发委员会相协调，定义出联邦政府的研发计划，包括 IT 安全研究领域的短期项目（1~3 年）、中期项目（3~5 年）以及长期项目（5 年或更长）。
R4-9	联邦政府资助的 2004 财年短期 IT 安全研发项目应当包括 OSTP 和研发委员会确认的优先项目。当前的优先项目包括入侵检测、Internet 基础设施安全（包括 BGP、DNS 等协议的安全）、应用程序的安全、拒绝服务、通信安全（包括 SCADA 系统的加密和鉴别）、高保障系统、安全的系统构成。

续表

R4-10	私营部门应该考虑在短期的优先研发项目中加入对高度安全和可信的操作系统的研究。如果该系统得以开发并成功通过了评估，则联邦政府应推动对这些系统的采购。
R4-11	联邦以及私营部门赞助的研发项目中均应包括对新兴技术的安全事项进行审查的项目。
R4-12	联邦政府各部及其各个机构必须特别注意无线技术中的安全风险。机构内应当考虑安装可持续对网络中的非授权连接进行检查的系统。它们应当仔细阅读 NIST 最近发布的无线技术报告，并充分研究 NIST 的建议和结论。在这个问题上，各机构的政策和流程应反映出该机构已经认真考虑了下列各种用于降低风险的措施：强加密、双向鉴别、屏蔽技术及其他的技术性安全对策、配置管理、入侵检测、事件处理以及计算机安全教育和意识培养项目。
R4-13	政府和工业界应当积极地促进个人、企业以及政府对无线技术，尤其是 802.11b 及相关标准的无线技术中的安全问题的意识。工业界和政府应密切合作，共同提高具有内建的透明安全性的无线 LAN 的改良标准及协议的不断发展。
R4-14	通过一场由工业界领导的国家级自愿活动，我们将建立起一个交换和交流中心，以推动软件补丁的更有效的实施。该活动还包括广泛交换当软件补丁对通用软件系统造成影响时的有关数据，在必要时，其中还要涉及对软件补丁的测试结果。
R4-15	软件工业应考虑在其产品的安装和实现中推行更安全的预设工作，包括：（1）促进用户对产品中的安全性的意识；（2）增强安全功能的易用性；（3）在方便时推广工业界的相关指南和最佳的操作方法，以对上述事项提供支持。
R4-16	发起国家级的公共-私营合作，宣传最佳操作步骤和方法学，提高软件代码开发中的完整性、安全性和可靠性。其中还包括有关的过程及流程，用于降低在软件开发中引入错误代码、恶意代码以及陷门的可能性。
R4-17	PCIPB 下属的意识培养委员会应与各部门的领导机关合作，培育一种公共-私营合作联盟，开发和传播网络空间安全方面的意识培养材料，如面向不同读者的工具以及每年一次的意识培训项目。
R4-18	“在线安全”运动应加以扩展，向其中加入面向不同听众群体的国家层次的广而告之节目。还应开发供各学校和公司使用的有关教育和培训材料。
R4-19	各州应考虑在州立大学中建立服务奖学金项目，资助大学生和研究生之中从事 IT 安全专业且愿意为州政府服务的学生。已有的服务奖学金项目要扩展到更多的学校，既向学生提供资助，也要发展教职员工。为使服务奖学金项目能够面向社区学院，还要继续增加教职员，并努力使该项目得到发展。
R4-20	CIO 委员会以及拥有网络空间安全培训专家的各联邦机构应考虑建立网络空间学会，把联邦政府的网络空间安全和计算机取证学方面的培训项目联合起来。
R4-21	国家之中各类公共或私营的实验室应通过建立与能源部 Sandia 国家实验室网络空间防御者项目相类似的项目而尽可能获益。
R4-22	PCIPB 下属的培训委员会应尽可能通过建立一支横跨多个联邦部门的 IT 和网络空间安全专家队伍而获益，尽最大可能充分利用那些颇具创新性的高效且灵活的人力资源项目的优势。
R4-23	州、地方和私营机构应考虑为小学和中学学生制定网络空间道德规范以及安全防护方面的项目和指南。
R4-24	IT 安全专家和有关协会与机构应努力研究设立严格的认证项目的方法和可行性，包括继续教育和重新考试项目。
R4-25	国会和行政部门应通过合作来为公共部门和私营部门之间围绕网络空间安全和基础设施脆弱性的信息的共享扫清障碍。
R4-26	某些负责的联邦机构应当制定一项战略，鼓励公民和企业上报网络空间发生的犯罪、攻击以及非授权入侵事件。除此之外，该战略还要探究可促进事件报告工作的相关机制。

续表

R4-27	FBI 和特工处应继续改善其对区域办公室的网络空间犯罪调查活动的协调，并考虑对示范联合任务组进行扩展。
R4-28	改善联邦、州和地方执法界中负责关键基础设施和网络空间安全事务的机关之间以及它们同其他机构和私营部门之间的信息共享和调查协调工作。
R4-29	联邦政府应当收集网络空间受害者（商行、组织以及个人）的调查数据，以更好地建立对安全问题的基本认识，并可衡量后续行动的有效性。
R4-30	联邦政府应审查联邦、州和地方执法机关在解决关键基础设施事件和网络空间犯罪时，在犯罪取证和事件调查方面所接受的培训及基金资助的水平。
R4-31	联邦政府应该不断评估政府的判决方针，审查其是否足够适用于网络空间犯罪。
R4-32	PCIPB 应与 OMB（管理和预算办公室）密切工作，并同私营部门和州政府保持合作，审查联邦和州政府的法律法规中哪些会阻碍市场推动力对网络空间安全的促进作用。
R4-33	PCIPB 的金融和银行信息基础设施委员会（FBHIC）要与保险工业合作，研究如何在网络空间安全中制定出有效的风险转移机制，包括改善风险建模的方法以及促进受损数据的可用性。
R4-34	机构应考虑每年公布如下信息：向该机构实施 IT 安全审计的公司的身份以及审计工作的总体状况、机构和董事会所控制的 IT 安全系统状况、机构对 IT 安全最佳实践措施或标准的遵循情况、机构在信息共享和分析中心（ISAC）以及其他 IT 安全项目中的参与情况。
R4-35	PCIPB 应与内部审计师学会、董事协会以及其他类似组织相合作，不断促进意识培养项目及最佳实践措施的有效性。
R4-36	行政部门应经常同隐私提倡者、工业界代表以及其他感兴趣的组织相协商，推动国家战略在实施中考虑隐私和公民自由问题，在加强网络和主机安全的同时要实现隐私的保护方案。
R4-37	作为联邦各部中年度安全审计的一部分，应审查在 IT 中对隐私条例的遵循性。
R4-38	相关的联邦机构应审查与《Gramm, Leach, Bliley 金融现代化法》以及《健康保险可行责任法》的实施有关的安全问题。
R4-39	ISP、软硬件提供商、IT 安全相关公司、计算机应急响应小组（CERT）、信息共享和分析中心（ISAC）应彼此合作，考虑建立一个实体或虚拟的网络运行中心（NOC），以便于信息共享，确保彼此间的协调，从而支持美国 Internet 运行的安全性和可靠性。虽然 NOC 可能不是一个政府所属的实体，由一个私营界的委员会负责管理，联邦政府应该努力寻求与其合作的途径。
R4-40	联邦政府应当在政府和非政府中与网络空间安全有关的核心网络运行中心内安装网络预警和信息网（CWIN），以供传播分析和预警信息，并负责完成危机协调工作。
R4-41	在与联邦政府的自愿性合作联盟中，工业界应制定并时常更新其网络空间安全危机应急计划，包括 Internet 功能的恢复计划。
R4-42	联邦政府应当审查已有的应急处理管理机关，并判断这些现有的机关是否能为 Internet 的恢复提供必要的支持。
R4-43	美国应建立一个强有力的反情报项目，以对抗美国政府、工业界、大学中的站点所面临的基于网络空间的情报收集活动。
R4-44	国家安全委员会应领导一项研究项目，在执法机构、国家安全机构、国防机构之间，改善对重大攻击的事件响应协调过程的认识。
R4-45	美国应当不断提高其能力，使国家能够迅速定位威胁性攻击或行为源，并能在攻击发生前便可将威胁加以遏制。

续表

R4-46	当某些国家或恐怖主义集团通过网络空间的攻击威胁到美国的核心利益时，美国将保留以必要的方式对该攻击做出响应的权力。
R4-47	公共-私营合作联盟应确认以网络和物理形式存在的各部门之间的互依赖性，并与《国土安全国家战略》协同，制定各项相关计划来消除与互依赖性相关的脆弱性。国家基础设施仿真和分析中心应支持上述工作。
R4-48	信息系统网络和网络数据中心的业主和操作者们应考虑制定修复和应急计划，以减轻这些网络的支撑设施在遭到大规模物理破坏时引发的后果。在需要时，联邦政府可以对这些工作进行协调，并提供技术援助。
R4-49	信息系统网络的业主和操作者们应当在必要时与联邦政府在自愿的基础上进行合作，制定适当的流程，以限制对关键设施的访问。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体的特定的、不断变化的环境	
讨 论	
需要进一步分析、争议和讨论的重点问题	
D4-1	政府、工业界和学术界应如何解决那些对网络空间的业主和操作者来说重要、有益，但又没有一个组织有足够的动力去关注的诸多问题？
D4-2	路由器的带外管理如何在 Internet 上实现？成本及收益各为几何？
D4-3	私营部门如何使推广项目覆盖 DCS/SCADA 用户界的所有层面，以提高人们对于脆弱性、事件后果以及事件减缓措施的意识？
D4-4	在推广项目中，DCS/SCADA 用户应当接受哪些培训课程和材料，以培养必需的安全技能？
D4-5	联邦的研发基金赞助下的已有的技术、设备或功能要应用到满足公共和私营部门的需求之中去，这种技术转化过程必须得到强化。而技术转化过程中最重要的则是私营部门对安全新技术的采用，尤其是提供商们对这些新技术的采用。它们应成为公共-私营合作联盟中讨论的主题之一。那么，有哪些机制可以有效地鼓励提供商们去采纳现有的以及新兴的安全技术？
D4-6	新兴技术，如无线局域网对安全和隐私的潜在影响有哪些？
D4-7	政府是否应与新兴技术的产品提供商密切合作，以促进提供商去披露其产品在使用中的脆弱性，并鼓励提供商将安全属性设计得对一般用户来说更加简便？
D4-8	软件工程学课程应该如何以及通过哪些途径做出改变，以反映出更安全的代码编制方法。
D4-9	对于系统的打补丁操作，是否有合适的方法来为其定义出标准的时间限度？
D4-10	应如何去衡量各级听众所接受到的安全意识培养？如何去衡量网络空间安全预警的有效性？
D4-11	在增强网络空间安全意识方面，私营部门中的人士应扮演何种角色？
D4-12	政府和私营工业界应如何建立有关项目来尽早选择出对 IT 安全工作有兴趣和/或富有安全才干的学生？如何鼓励和发展他们的兴趣和技能？如何指导他们步入工作岗位？
D4-13	政府和工业界如何确立国家级的网络空间安全专业培训和教育标准，以满足美国机构的需求？
D4-14	是否应创建一个认可机构，使其为系统管理员级的安全知识需求设定基础的标准？
D4-15	其他级别的 IT 安全专业是否应考虑设置对等的认证或认可项目？
D4-16	联邦政府是否应向 ISAC 提供支持，如基金、技术工具或设备？
D4-17	需要多少受害者权力组织才能针对网络空间犯罪可能带来的危险起到更强有力的意识宣传作用？
D4-18	在联邦、州和地方的网络空间犯罪法律之间是否存在鸿沟？如果是，这种鸿沟会带来何种影响？
D4-19	我们能从“巴塞尔协定”中吸取哪些有可能会增强其他基础设施安全性的知识？
D4-20	信息披露有可能给攻击者以可乘之机，那么，是否应该审查州和联邦政府对于信息披露的需求？

续表

D4-21	如何鼓励工业界在其规划和产品之中通过灵活的、非受控的方法加入必要的隐私保护手段？
D4-22	政府机构应如何合作来推动司法界中隐私问题的协调？
D4-23	联邦政府和私营工业应如何培养有关人员去“深度挖掘”数据并检测攻击模式的能力？
D4-24	对于传统威胁以及核威胁，需要用四个十年来发展迹象发现和预警能力，当美国要对抗破坏性颇高的网络空间威胁时，应如何发展一种类似的“迹象发现和预警”体系结构？
D4-25	是否需要有一个新的权威机关（不止在备战和国防领域）来负责为关键基础设施管理产品和服务的优先交付？
D4-26	确认关键基础设施互依赖性时需要公共和私营部门之间的积极讨论。应建立怎样的一种过程来帮助联邦政府为互依赖性和脆弱性的研究排定优先次序并提供基金？
D4-27	网络空间攻击可以从世界上任何地方发起，因此很有必要发展一种能够快速定位攻击源的能力，以有效响应安全事件。这种功能通常被称为“归因”，它对于判断出某次攻击是否由国外势力所发起是极为重要的。那么，政府和工业界的分析师应该如何增强其归因能力，以更加快速地定位攻击源？
D4-28	国家安全界应如何强化反情报方面的培训，以更好地支持网络空间安全？

## 9. 第5级：全球

我们的战略目标是与国际社会相合作，确保美国的关键性经济和国家安全基础设施所依赖的全球信息基础设施的完整性。该目标要通过一系列活动来实现。美国政府为此将：

- 推动一个国际化合作网络的发展，在安全事件初露端倪时便能通过该网络对其确认并提供防护。
- 鼓励所有的国家都能发布足够的网络空间安全法律，以利于美国执法机关能向我们国家及国家利益所遭到的网络空间犯罪行为发起调查和起诉，不论该犯罪行为是源于国内还是国外。
- 与国际组织相合作，以培育广泛的“安全文化”，确保全球信息基础设施的长久安全。
- 推动国际社会采纳可保障全球信息基础设施安全性的国际性通用技术标准。

### 问题和挑战

美国对推动网络空间安全的兴趣已经远远超越了其国界。其关键的国内信息基础设施均有与加拿大、墨西哥、欧洲、亚洲和南美的直接连接，国家的经济与安全依赖于遍布全球的美国企业、军事力量以及国外的贸易伙伴；而反过来，上述机构同样也需要依赖于安全可靠的信息网络来工作。大量的网络空间攻击来源于国外的系统，或经由国外系统，甚至跨越了多个国界，我们需要国际合作来打击这些攻击。

1998 年发生的一次事件为美国政府敲响了国家安全的警钟。在这个最终被称为“Solar Sunrise”的事件中，美国的军事系统遭到了电子攻击。从现象上看，攻击来自于阿联酋境内的计算机系统。在当时，由于伊拉克没有遵循联合国大规模杀伤武器核查小组的要求，美国正考虑对伊拉克采取军事行动，而恰在这个时候，美国军队的管理和部署所依赖的无密级的后勤、管理和会计系统在同一时刻遭到了攻击。在这种时候发生的攻击事件使美国怀疑，这是敌对国家发起的第一波大规模网络空间攻击行动。

而最后，我们发现这是两个加利福尼亚少年在一名熟练的以色列黑客指导下的所为，而这名以色列黑客本身也是一位少年。而且他们使用的是 Internet 上得到的黑客工具。为了隐藏其形迹，他们是通过国外计算机进行连接的。可见，即使是美国人对美国的计算机实施的攻击，其中也常常有国际因素。

另一个能够展现全球经济威胁的事件就更加鲜明了。2000 年 2 月初，Internet 上的几个最大的商业 Web 站点上的计算机服务器被无数的连接请求所淹没，导致系统遭到阻塞，服务器资源被消耗完毕。最终，这些分布式拒绝服务（DDoS）攻击使大部分 Internet 遭遇瘫痪。通过美国与加拿大探员之间的密切合作，我们才发现这是一名加拿大少年在“黑手党男孩”的名号下干的。他在数月之内入侵了世界上多台计算机，始终保持着对这些受害服务器的控制权，因此他就相当于创建了一支“僵尸军队”，这支军队可以在其指挥下淹没下一个受害者的服务器。这次事件中，系统由于性能的降低和中断所导致的经济损失据估计超过了 10 亿美元。

而仅仅几个月之后，在 2000 年 5 月 4 日的清晨，“我爱你”病毒开始大肆感染全球的计算机。在亚洲首先发现该病毒后，“我爱你”迅速扫荡了全世界，对政府和私营部门网络的攻击成泛滥之势。到人们控制住“我爱你”之前，它已经感染了将近 6 000 万台计算机，造成了数十亿美元的损失。全世界的执法机关合作起来去搜寻攻击者，最终发现菲律宾的一名计算机科学系的辍学学生是始作俑者。然而他并未因此而遭到起诉或惩罚，因为在当时，菲律宾法律中还没有对这类行为明确地定罪。

总的来说，这些事件清楚地表明，只靠美国国内的努力还不能足以制止或预防他们。我们必须与国际伙伴密切合作，通过合作机制来预防这些攻击所导致的破坏。如果在预防环节上未能成功，我们还可以借此对犯罪行为展开调查和起诉。

## 战略讨论

美国将推行一系列活动来强化其全球性的网络空间安全，在必要时通过各种双边、多边以及国际论坛来传播其核心的政策信息。这些活动将：建立起实时地、全天候的观察和预警网络，发现并阻止安全事件；在每个国家都建立并连接一个网络空间安全协调员网络；通过国际机构来推动那些对建立全球网络空间安全文化至关重要的原则和标准的区域性发展；协助各国制定法律并增强技能，以对跨国的网络空间犯罪行为实施有效的调查和起诉；联合全世界最优秀的思想，共同研究长期的网络空间安全解决方案。

## 加强国际合作

### （1）威胁管理

过去 3 年，美国已经就网络安全空间问题同其他国家打过交道，这些工作还要进一步扩展，以确保网络空间安全事件的预防方面的国际合作能够走上正轨。我们将鼓励各国建设其自己的观察和预警网络，当攻击或病毒事件迫在眉睫时，能够使政府机构、公共部门以及其他国家得到通知。为促进威胁信息的实时共享，美国将建立起一个国家化网络，在全球范围接收、评估、并传播这类信息。该网络将建立在很多非政府机构的功能之上，如事件响应和安全小组论坛（FIRST）以及一些有悠久历史的国际电信机构，包括国际电联（ITU）。在后者中，几乎每个国家都是其成员，它还包括 600 多个私营部门的组织。

#### ①国家网络空间协调员

美国主张每个国家都从千年虫事件中吸取经验，指定一个集中化的联系地址，在本国与全球的网络空间安全工作之间承担联络角色。这些联系地址的建立将极大地加强网络空间安全方面的国际合作与问题的解决。



## ②北美网络空间安全

本战略中将特别强调把北美建设成“安全的网络空间地带”。要与加拿大和墨西哥相合作，制定最佳实践措施，以保护电信、能源、运输、银行与金融系统、应急服务、食品、公共健康、供水所依赖的共享且互联的信息网络的安全。美国将寻求协调的解决方案，确保美国人民的生活中的那些关键系统的完整性和可靠性。

## ③通过国际组织实现合作

## (2) 打击网络空间犯罪

美国将积极培育网络空间犯罪的调查和起诉方面的国际合作机制。很多现行的多边工作，如八国集团、亚太经合论坛（APEC）、欧洲合作和发展组织、欧洲委员会等组织均将对该领域的成功起到重要作用。对于这些组织制定的建议和行动计划，美国将在同意的基础上加以实施。上述组织的活动中，美国尤其将鼓励更多的国家加入全时运行的高科技犯罪联络网，该网络最早始于八国集团，现已扩展到了欧洲委员会以及其他国家之中。

美国已于最近签署了《欧洲委员会网络犯罪大会约定》，并表明了对该约定的支持。这一约定要求各国将网络空间攻击视为确凿无疑的犯罪行为，并通过采取流程措施以及相互间协助来更好地打击国际间的网络空间犯罪。美国将鼓励更多的国家能接受这份约定，或至少要使这些国家的法律与这些要求相一致。

## (3) 建设安全网络的工作

为确保信息系统的安全性，并促进重要知识的共享，美国将参与一系列合作工作，解决在保障信息网络的完整性过程中遇到的各种技术的、科学的以及政策的问题。主要活动将包括鼓励制定和采纳国际技术标准，并促进世界上最优秀的科学家和研究者之间的合作和研究。

美国还将通过很多努力来在新的信息社会的所有参与者之间灌输“安全文化”，如 OECD（欧洲合作和发展组织）的《信息系统和网络安全指南》。

大多数国家的关键信息基础设施掌握在私营部门手中，所以美国将鼓励其工业界参与上述工作，同其国外同行展开对等的对话，从而达到一举两得的目的：取得网络空间安全方面的有效案例；展现网络空间安全中与政府合作的成功途径。

工作安排	
第 5 级：全 球	
建 议	
政府与非政府实体可采取的用于增进网络安全的具体行动	
R5-1	在与私营部门的协调下，联邦政府应同世界各国以及各非政府和国际组织相合作，建立国家和国际级的观察和预警网，以检测和预防网络空间的攻击。此外，该网络还有助于对攻击的调查和响应提供支持。
R5-2	美国政府应鼓励各国加入《欧洲委员会网络犯罪大会约定》，或至少确保这些国家的法律和执法流程要全面。
R5-3	美国政府应与加拿大和墨西哥合作，制定和执行最佳实践措施，以保护大量共享的关键性北美信息基础设施。
R5-4	在与工业界的合作联盟中，美国应通过国际组织中的工作来促进国外的公共部门以及私营部门之间就信息基础设施保护展开对话与合作，推动全球“安全文化”的建设。
R5-5	应鼓励每个国家都指派一名国家网络空间安全协调员。

续表

R5-6	美国应通过网络空间安全中研究和开发方面的合作，吸收全球的科学和技术精英。 这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体的特定的、不断变化的环境
行 动	
现有的网络安全工作	
P5-1	多边组织的发展：通过参加各种多边组织，如八国集团和欧洲委员会，美国已经在推动与他国的网络空间安全合作方面取得了长足的进步，且这种进步还将继续下去。
P5-2	支持 COE 约定：美国已经并将继续动员很多国家加入 COE 约定，或鼓励这些国家至少颁布其内容与 COE 约定一样全面的网络空间犯罪法律。
P5-3	双边讨论：通过双边讨论，美国鼓励各国改善其法律体系并发展网络空间犯罪领域中预防、调查和起诉方面的双边合作。美国因此而大大促进了其他国家网络空间安全以及这些国家同美国执法工作之间的合作。
P5-4	咨询和教育推广：美国已经建议一些国家制定网络空间犯罪法律，且针对一个健全的网络空间法律体制所能发挥的重要作用而开展了各种教育讨论班。美国还向国外执法机关提供了培训和技术援助，以提高它们在打击网络空间犯罪方面的协作能力。
P5-5	国际观察和预警网：美国参与了很多旨在对跨越国际边界的网络空间攻击事件进行早期检测和预防的国际化网络，其中一个就是由国家基础设施保护中心（NIPC）建立的。
P5-6	国际执法网络：美国参与了很多旨在对跨越国际边界的网络空间攻击事件进行调查并起诉入侵者的国际化网络，如由八国集团维护的“国际高科技犯罪 24 小时联系处”
讨 论	
需要进一步分析、争议和讨论的重点问题	
D5-1	为了更好地协助发展中国家建立“安全文化”，私营部门应当扮演何种角色？

## 10. 建议概要

第 1 级：家庭用户和小型商业	
R1-1	由于自动化的黑客程序能够对 Internet 进行扫描并找到未受保护的宽带连接，计划安装 DSL 或电缆 Modem 的家庭用户和小型商业应该考虑安装防火墙（某些 ISP 在为用户安装 DSL 或电缆 MODEM 时提供防火墙软件）。一旦安装了防火墙软件，就必须定期访问该厂商的站点并对软件进行及时更新。
R1-2	由于每周都有新病毒出现，家庭用户和小型商业应确保运行及时更新的防病毒软件（某些防病毒软件提供商提供在线自动升级服务。某些 ISP 对所有接收到的电子邮件进行病毒扫描，随后才将它们发给用户）。
R1-3	由于新病毒通常以电子邮件的方式传播，家庭用户应该在打开来自未知发送方的电子邮件（尤其是当这些电子邮件带有附件）时保持谨慎。为减少来自未知发送方的电子邮件，家庭用户应该使用有关软件来拒收被称为“spam”的广告电子邮件（某些 ISP 提供能够使 spam 失效的程序。某些 ISP 提供允许用户拒收发送方不在朋友或者经选择的联系人之列的所有电子邮件）。
R1-4	为了增强计算机的安全，家庭用户也应该通过访问厂商站点的方式定期更新各自的计算机操作系统（如 Microsoft Windows 和 Linux）和主要的应用软件（这些软件被用于进行 Internet 浏览或者创建文件、图表等）。（某些厂商提供在线自动升级。）
R1-5	ISP、防病毒软件公司和操作系统/应用软件开发商应该考虑进行合作，以便家庭用户和小型商业能够更便捷地获得安全软件（并且对其及时进行自动升级），包括有关软件升级与新补丁的警告信息

续表

第 2 级：大型机构	
R2-1	CEO 应考虑成立机构安全委员会，负责整体考虑本机构的网络安全、物理安全和可操作性。
R2-2	CEO 应考虑采用常规的独立性信息技术安全审计、修补流程，以及对最佳实践措施的审查。
R2-3	公司董事会应考虑成立信息安全董事会委员会，应确保 CEO 定期仔细审阅公司主要信息安全官员的建议。
R2-4	应定期审查和演练公司信息技术持续计划，应考虑站点和人员的更换。为消除风险，应考虑采用不同信息设备提供商的产品。
R2-5	公司应考虑主动参与业界活动，以便做到：（1）为同行公司开发最佳的信息技术安全实践措施和采购标准；（2）通过合适的信息共享和分析中心（ISAC）共享信息技术安全信息；（3）增强网络安全意识与对于公共政策问题的考虑；（4）与保险业进行合作，扩大保险在管理网络风险方面的作用。
R2-6	公司应该考虑加入公共-私营部门合作组织，以便建立一个奖励计划，对为网络安全做出突出贡献的机构进行奖励。
R2-7	（1）机构应该审查大型机安全软件和程序，以便确保本机构利用了有效的技术和流程措施；（2）信息技术经销商和采用大型机服务器的机构应该考虑进行合作，以便对大型机安全设备进行审查和升级，以及确保本机构继续拥有足够多经培训的主流产品应用领域内的专家；（3）信息安全审计应该包括对于主流产品的综合性评估
第 3 级：关键部门	
联邦政府	
R3-1	以增强对更安全的产品的采购为目的，联邦政府将在 2003 财年第四季度之前完成对国家信息保障计划（NIAP）的综合考查，以便做到：确定 NIAP 的成本有效性并找出其中的安全不足；判断 NIAP 是否为消除这些安全不足而确定了发展目标，是否正在试图实现这一目标，并判断 NIAP 的改进、优化、扩充工作的适宜性及成本有效性。
R3-2	在 2003 财年第三季度结束之前，联邦政府将确定是否应该要求为联邦政府提供安全服务的私营部门通过某种最低能力程度的资格认证。
R3-3	通过采用电子政府模型，在 2003 财年第三季度结束之前，联邦政府将通过在政府内部更广泛地采办、运行和维护安全工具与安全服务而获得益处（包括减少小型机构的资源压力）。
R3-4	通过正在进行的 E-Authentication 行动，在 2003 财年第二季度结束之前，为促进部门间的一致性与互操作性，联邦政府将扩大所有能够采取相同的物理与逻辑访问控制工具和鉴别机制的部门范围。
R3-5	联邦政府部门应该继续扩大自动化的机构安全评测和安全政策实施工具的应用程度，并为免受攻击而积极采用威胁管理工具。2003 财年第二季度结束之前，联邦政府将针对是否有必要采取具体行动以便进一步促进这些工具的使用进行决策。
R3-6	联邦政府将评估在服务中断时各种应急替代方案的可行性和成本有效性，如 VPN、专网等。
R3-7	联邦政府应带头采用安全网络协议。联邦政府应该在安全协议发布之初即考虑该协议是否消除了某个安全脆弱性，以及该协议的应用是否能够对联邦政府的网络运行和安全状况产生性价比合理的影响。
R3-8	2003 财年第二季度结束之前，联邦政府将选择一个机构，考查安全和应急战备演习的成本有效性。演习中发现的脆弱性将列入机构的 GISRA 矫正计划中。
R3-9	OMB 将与 CIO 委员会进行合作，在遵循事实的基础上确定是否应该为整个联邦政府的安全测量而成立一个领导机构。可供选择的现有机构包括 GSA、NIST、国土安全部、国防部
第 3 级：关键部门	
州和地方政府	
R3-10	州和地方政府应当考虑为其下属各机构建立 IT 安全项目，包括意识培养、审计、和标准。州、地方和城市协会应考虑提供相关的援助、资料以及示范项目。
R3-11	州和地方政府应当考虑参与已建立信息共享和分析中心（ISAC）。
R3-12	州和地方政府应当考虑扩展其面向执法官员的计算机犯罪培训项目，这些官员包括法官、检察官以及警察。联邦政府可以提供有关援助，对培训项目提供协调，并考虑在必要时提供资金方面的帮助

续表

第 3 级：关键部门	
高等教育	
R3-13	每个学院和大学都应考虑建立在任何时候均可以联系到的联络点，当学校的 IT 系统被发现正在发起拒绝服务攻击时，能够让 ISP 和执法官员与学校保持联络。
R3-14	学校和大学应当考虑建立：（1）一个或多个信息共享和分析中心（ISAC），用以对付网络空间攻击和脆弱性；（2）示范性的指南，授予首席信息官（CIO）处理网络空间安全的权力；（3）一套或多套 IT 安全最佳实践措施文档；（4）示范性的用户意识培养项目和资料
第 3 级：关键部门	
私营部门	
R3-15	每个基础设施部门都应考虑建立一个信息共享和分析中心（ISAC），并与其他 ISAC 保持协作。联邦政府将考查根据需把各个 ISAC 与适当的网络安全预警和分析中心相联的情况，并将促进在必要时对关键基础设施保护信息的提供。
R3-16	每个关键基础设施部门都应该考虑针对技术缺陷以及研发缺陷实施分析，与科技政策办公室（OSTP）的工作相协作，为联邦政府网络空间安全研究排定优先级，以解决这些技术和研发中存在的缺陷。各关键基础设施部门和 OSTP 应当在这些研究活动的实施中保持协调。
R3-17	每个关键基础设施部门应当考虑制定网络空间安全的最佳实践措施，并在必要时提供安全的 IT 产品和服务采购的方针指南。
R3-18	每个关键基础设施部门应当考虑部门内的彼此合作，以实施面向具体部门的信息安全意识培养运动。
R3-19	每个关键基础设施部门应当考虑建立网络空间安全应急响应的互助计划。司法部和联邦贸易委员会将与各基础设施部门共同工作，以解决互助合作中出现的任何壁垒
第 4 级：国家的优先任务	
保护 Internet 机制	
R4-1	公共-私营合作联盟应当优化并促进边界网关协议、IP、DNS 及其他协议对改良的安全特性的吸收。
R4-2	公共-私营合作联盟应当完善并促进对更安全的路由技术和管理技术的吸收，如带外管理。
R4-3	从第一级公司开始的 Internet 服务提供商或大型的接入提供商应当考虑采纳“最佳操作规则”来管理其涉及网络空间安全的行为，包括与其他公司之间开展的与安全事项有关的合作。
R4-4	公共-私营合作联盟应当确认并解决基础性的 Internet 技术需求，这其中有可能要利用已有的项目，也许还要为这些活动建立基金
第 4 级：国家的优先任务	
DCS/SCADA	
R4-5	公共-私营合作联盟应当制定最佳实践措施并发展新技术，以增强 DCS（数字控制系统）和 SCADA（监督控制和数据采集）系统在公共事业、制造业及其他网络中的安全性，此事应被置于极高的优先级。
R4-6	政府和工业界应该合作确定最为关键的 DCS/SCADA 相关场所，并为这些场所制定一个优先级已经得到排序的安全改善计划。DCS/SCADA 用户应考虑采纳能源部的文献《提高 SCADA 网络安全性的 21 个步骤》
第 4 级：国家的优先任务	
研究和开发	
R4-7	PCIPB 的研发委员会应针对现有的推广机制、学术界和工业及政府界间的研发活动的确定和协调而实施综合性的审查和缺陷分析。在 2003 年 2 月，委员会应完成上述工作，并向 PCIPB 提交其建议书，对上述机制的实现、扩展及建设提出建议。
R4-8	PCIPB 应负责在每年度与科技政策办公室（OSTP）主任和 PCIPB 下属的研发委员会相协调，定义出联邦政府的研发计划，包括 IT 安全研究领域的短期项目（1~3 年）、中期项目（3~5 年）以及长期项目（5 年或更长）。

续表

R4-9	联邦政府资助的 2004 财年短期 IT 安全研发项目应当包括 OSTP 和研发委员会确认的优先项目。当前的优先项目包括：入侵检测、Internet 基础设施安全（包括 BGP、DNS 等协议的安全）、应用程序的安全、拒绝服务、通信安全（包括 SCADA 系统的加密和鉴别）、高保障系统、安全的系统构成。
R4-10	私营部门应该考虑在短期的优先研发项目中加入对高度安全和可信的操作系统的研究。如果该类系统得以开发并成功通过了评估，联邦政府应推动对这些系统的采购。
R4-11	联邦以及私营部门赞助的研发项目中均应包括对新兴技术的安全事项进行审查的项目
第 4 级：国家的优先任务	
保护新兴系统的安全	
R4-12	联邦政府各部及其各个机构必须特别注意无线技术中的安全风险。机构内应当考虑安装可持续对网络中的非授权连接进行检查的系统。它们应当仔细阅读 NIST 最近发布的无线技术报告，并充分研究 NIST 的建议和结论。在这个问题上，各机构的政策和流程应反映出该机构已经认真考虑了下列各种用于降低风险的措施：强加密、双向鉴别、屏蔽技术及其他的技术性安全对策、配置管理、入侵检测、事件处理以及计算机安全教育和意识培养项目。
R4-13	政府和工业界应当积极地促进个人、企业以及政府对无线技术，尤其是 802.11b 及相关标准的无线技术，中的安全问题的意识。工业界和政府应密切合作，共同提高具有内建的透明安全性的无线 LAN 的改良标准及协议的不断发展
第 4 级：国家的优先任务	
脆弱性矫正	
R4-14	通过一场由工业界领导的国家级自愿活动，我们将建立起一个交换和交流中心，以推动软件补丁的更有效的实施。该活动还包括广泛交换当软件补丁对通用软件系统造成影响时的有关数据，在必要时，其中还要涉及对软件补丁的测试结果。
R4-15	软件工业应考虑在其产品的安装和实现中推行更安全的预设工作，包括：（1）促进用户对产品中的安全性的意识；（2）增强安全功能的易用性；（3）在方便时推广工业界的相关指南和最佳的操作方法，以对上述事项提供支持。
R4-16	发起国家级的公共-私营合作，宣传最佳操作步骤和方法学，提高软件代码开发中的完整性、安全性和可靠性。其中还包括有关的过程及流程，用于降低在软件开发中引入错误代码、恶意代码以及陷门的可能性
第 4 级：国家的优先任务	
意识培养	
R4-17	PCIPB 下属的意识培养委员会应与各部门的领导机关合作，培育一种公共-私营合作联盟，开发和传播网络空间安全方面的意识培养材料，如面向不同读者的工具以及每年一次的意识培训项目。
R4-18	“在线安全”运动应加以扩展，向其中加入面向不同听众群的国家层次的广而告之节目。还应开发供各学校和公司使用的有关教育和培训材料
第 4 级：国家的优先任务	
培训和教育	
R4-19	各州应考虑在州立大学中建立服务奖学金项目，资助大学生和研究生之中从事 IT 安全专业且愿意为州政府服务的学生。已有的服务奖学金项目要扩展到更多的学校，既向学生提供资助，也要发展教职员工。为使服务奖学金项目能够面向社区学院，还要继续增加教职员，并努力使该项目得到发展。
R4-20	CIO 委员会以及拥有网络空间安全培训专家的各联邦机构应考虑建立网络空间学会，把联邦政府的网络空间安全和计算机取证学方面的培训项目联合起来。
R4-21	国家之中各类公共或私营的实验室应通过建立与能源部 Sandia 国家实验室网络空间防御者项目相类似的项目而尽可能获益。

续表

R4-22	PCIPB 下属的培训委员会应尽可能通过建立一支横跨多个联邦部门的 IT 和网络空间安全专家队伍而获益，尽最大可能充分利用那些颇具创新性的高效且灵活的人力资源项目的优势。
R4-23	州、地方和私营机构应考虑为小学和中学学生制定网络空间道德规范以及安全防护方面的项目和指南
第 4 级：国家的优先任务	
认证	
R4-24	IT 安全专家和有关协会与机构应努力研究设立严格的认证项目的方法和可行性，包括继续教育和重新考试项目
第 4 级：国家的优先任务	
信息共享	
R4-25	国会和行政部门应通过合作来为公共部门和私营部门之间围绕网络空间安全和基础设施脆弱性的信息的共享扫清障碍
第 4 级：国家的优先任务	
网络空间犯罪	
R4-26	某些负责的联邦机构应当制定一项战略，鼓励公民和企业上报网络空间发生的犯罪、攻击以及非授权入侵事件。除此之外，该战略还要探究可促进事件报告工作的相关机制。
R4-27	FBI 和特工处应继续改善其对区域办公室的网络空间犯罪调查活动的协调，并考虑对示范联合任务组进行扩展。
R4-28	改善联邦、州和地方执法界中负责关键基础设施和网络空间安全事务的机关之间以及他们同其他机构和私营部门之间的信息共享和调查协调工作。
R4-29	联邦政府应当收集网络空间受害者（商行、组织以及个人）的调查数据，以更好地建立对安全问题的基本认识，并可衡量后续行动的有效性。
R4-30	联邦政府应审查联邦、州和地方执法机关在解决关键基础设施事件和网络空间犯罪时，在犯罪取证和事件调查方面所接受的培训及基金资助的水平。
R4-31	联邦政府应该不断评估政府的判决方针，审查其是否足够适用于网络空间犯罪
第 4 级：国家的优先任务	
市场推动力	
R4-32	PCIPB 应与 OMB（管理和预算办公室）密切工作，并同私营部门和州政府保持合作，审查联邦和州政府的法律法规中哪些会阻碍市场推动力对网络空间安全的促进作用。
R4-33	PCIPB 的金融和银行信息基础设施委员会（FBIIC）要与保险工业合作，研究如何在网络空间安全中制定出有效的风险转移机制，包括改善风险建模的方法以及促进受损数据的可用性。
R4-34	机构应考虑每年公布如下信息：向该机构实施 IT 安全审计的公司的身份以及审计工作的总体状况、机构和董事会所控制的 IT 安全系统状况、机构对 IT 安全最佳实践措施或标准的遵循情况、机构在信息共享和分析中心（ISAC）以及其他 IT 安全项目中的参与情况。
R4-35	PCIPB 应与内部审计师学会、董事协会以及其他类似组织相合作，不断促进意识培养项目及最佳实践措施的有效性
第 4 级：国家的优先任务	
隐私和公民自由	
R4-36	行政部门应经常同隐私倡导者、工业界代表以及其他感兴趣的组织相协商，推动国家战略在实施中考虑隐私和公民自由问题，在加强网络和主机安全的同时要实现隐私的保护方案。
R4-37	作为联邦各部中年度安全审计的一部分，应审查在 IT 中对隐私条例的遵循性。
R4-38	相关的联邦机构应审查与《Gramm、Leach、Bliley 金融现代化法》以及《健康保险可携性和责任法（HIPAA）》的实施有关的安全问题

续表

第 4 级：国家的优先任务	
网络空间分析和预警	
R4-39	ISP、软硬件提供商、IT 安全相关公司、计算机应急响应小组（CERT）、信息共享和分析中心（ISAC）应彼此合作，考虑建立一个实体或虚拟的网络运行中心（NOC），以便于信息共享，确保彼此间的协调，从而支持美国 Internet 运行的安全性和可靠性。虽然 NOC 可能不是一个政府所属的实体，由一个私营界的委员会负责管理，联邦政府应该努力寻求与其合作的途径。
R4-40	联邦政府应当在政府和非政府中与网络空间安全有关的核心网络运行中心内安装网络预警和信息网（CWIN），以供传播分析和预警信息，并负责完成危机协调工作
第 4 级：国家的优先任务	
运营连续性、恢复和重建	
R4-41	在与联邦政府的自愿性合作联盟中，工业界应制定并时常更新其网络空间安全危机应急计划，包括 Internet 功能的恢复计划。
R4-42	联邦政府应当审查已有的应急处理管理机关，并判断这些现有的机关是否能为 Internet 的恢复提供必要的支持
第 4 级：国家的优先任务	
国家安全	
R4-43	美国应建立一个强有力的反情报项目，以对抗美国政府、工业界、大学中的站点所面临的基于网络空间的情报收集活动。
R4-44	国家安全委员会应领导一项研究项目，在执法机构、国家安全机构、国防机构之间，改善对重大攻击的事件响应协调过程的认识。
R4-45	美国应当不断提高其能力，使国家能够迅速定位威胁性攻击或行为源，并能在攻击发生前便可将威胁加以遏制。
R4-46	当某些国家或恐怖主义集团通过网络空间的攻击威胁到美国的核心利益时，美国将保留以必要的方式对该攻击做出响应的权力
第 4 级：国家的优先任务	
互依赖性和物理安全	
R4-47	公共-私营合作联盟应确认以网络 and 物理形式存在的各部门之间的互依赖性，并与《国土安全国家战略》协同，制定各项相关计划来消除与互依赖性相关的脆弱性。国家基础设施仿真和分析中心应支持上述工作。
R4-48	信息系统网络和网络数据中心的业主和操作人员应考虑制定修复和应急计划，以减轻这些网络的支撑设施在遭到大规模物理破坏时引发的后果。在需要时，联邦政府可以对这些工作进行协调，并提供技术援助。
R4-49	信息系统网络的业主和操作人员应当在必要时与联邦政府在自愿的基础上进行合作，制定适当的流程，以限制对关键设施的访问。
第 5 级：全球	
R5-1	在与私营部门的协调下，联邦政府应同世界各国以及各非政府和国际组织相合作，建立国家和国际级的观察和预警网，以检测和预防网络空间的攻击。此外，该网络还有助于对攻击的调查和响应提供支持。
R5-2	美国政府应鼓励各国加入《欧洲委员会网络犯罪大会约定》，或至少确保这些国家的法律和执法流程要全面。
R5-3	美国政府应与加拿大和墨西哥合作，制定和执行最佳实践措施，以保护大量共享的关键性北美信息基础设施。

续表

R5-4	在与工业界的合作联盟中，美国应通过国际组织中的工作来促进国外的公共部门以及私营部门之间就信息基础设施保护展开对话与合作，推动全球“安全文化”的建设。
R5-5	应鼓励每个国家都指派一名国家网络空间安全协调员。
R5-6	美国应通过网络空间安全中研究和开发方面的合作，吸收全球的科学和技术精英。
这些建议的可行性和成本有效性会在各实体间有所不同。在选择是否应用这些建议时，每个实体都应当考查该实体的特定的、不断变化的环境	



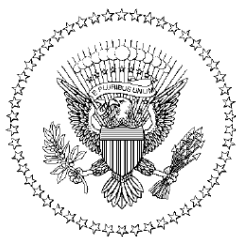
---

## 六、保护网络空间的国家战略

美国白宫

2003 年 2 月

---



华盛顿 白宫

我的美国同胞们：

美国的商业交易模式、政府的运行方式以及国防建设已经发生了改变，这些活动现在依赖于互联的信息技术基础设施网络，我们称其为网络空间。《保护网络空间的国家战略》为保护这一对我们的经济、安全和生活方式至关重要的基础设施提供了框架。

在过去几年，对网络空间的威胁急速上升，美国的政策是通过保护关键基础设施，防止信息系统的运行遭到破坏，从而保护美国的人民、美国的经济及国家的安全。在网络空间的脆弱性被用来破坏国家基础设施的网络支撑系统之前，我们必须减少这些脆弱性，确保将网络空间的破坏控制在频率小、跨时短、可控及损失尽可能小这样一个规模上。

保护网络空间是一项异常艰难的战略挑战，它需要整个社会，包括联邦政府、州和地方政府、私营部门以及美国人民付出协调一致且集中化的努力。为推动美国人民参与到保护网络空间的行动中来，本战略的草案版在此之前已经发布并征求公众的意见，全国也举办了十次市政会，以听取对这一国家战略的意见，成千上万的人和无数的机构参加了这些市政会并提出了建议，我在此对他们的积极参与表示感谢。

不论是现在还是将来，美国的网络空间安全战略的基石是公共-私营合作联盟。联邦政府呼吁公共-私营合作联盟的形成及各方的参与，共同实现本部战略。只有联合行动，我们才能在网络空间中建设一个更加安全的未来。

——布什

## 1. 执行摘要

我们国家的基础设施包括农业、食品、供水、公共健康、应急服务、政府、国防工业基地、信息与通信、能源、运输、银行与金融、化学品和危险物品、邮政和航运部门的公共和私营部门。网络空间则是其神经系统，是我们整个国家的控制系统，它由成千上万互联的计算机、服务器、路由器、交换机、光纤构成，他们是关键基础设施运行的基础。因此，网络空间的健康运行对我们的经济和国家安全至关重要。

《保护网络空间的国家战略》是保护国家的总体战略的一个要素，是《国土安全国家战略》具体实施的一个构成部分，并由《关键基础设施和重要资产的物理保护国家战略》所补充。本战略的目的是使美国人民能够保护其所拥有、运营、控制或交互的网络空间。保护网络空间是一个艰巨的战略性挑战，需要包括联邦政府、州和地方政府、私营部门及所有的美国人民在内的整个社会的协调一致且目标集中的努力。

《保护网络空间的国家战略》概括了组织工作和优先级工作的初步框架。它为参与保护网络空间的联邦政府部门和机构指明了方向，它还描述了州和地方政府、私营公司和组织以及每一位美国公民在改善我们共同的网络安全时必须采取的步骤。本战略强调了私营部门的角色，为所有美国人对自身所处的网络空间的保护提供了框架。网络空间的动态性要求对这一战略不断地进行调整和补充。

网络攻击的快速性和匿名性使得很难区分恐怖分子、犯罪分子和民族国家在网络上的行为，即使能够将他们区分出来，通常也是在事件发生之后。《保护网络空间的国家战略》则有助于减少我们国家的关键信息基础设施和支撑这些基础设施的资源面临攻击时的脆弱性。

### 战略目标

与《国土安全国家战略》相一致，《保护网络空间的国家战略》的目标是：

- 防止对美国关键基础设施的网络攻击。
- 减少国家对网络攻击的脆弱性。
- 在出现网络攻击时，尽量减少损失并缩短恢复时间。

### 威胁和脆弱性

我们的经济建设和国家安全完全依赖于信息技术和信息基础设施。我们依赖的信息基础设施的核心是 Internet，这个系统最初的设计是用于在科学家之间共享非涉密的研究成果，在当时认为这些用户不会滥用计算机网络。而如今，同样的这样一个 Internet 却连接着数百万个其他的计算机网络，是国家的大多数重要服务和基础设施正常运行的基础。这个计算机网络还控制着电力变压器、火车、输油管道、化学物品存储器、雷达、股市等，这些都是网络空间之外的东西。

一些恶意人员能够对我们的关键信息基础设施实施攻击，最受关注的是有组织的网络攻击能够破坏国家关键基础设施、经济建设并危害国家安全。实施这种攻击要求具有高超的技术，这从一定程度上解释了为什么到现在为止还很少出现这种攻击。但是我们不能太过乐观，当前已经有一些有组织的攻击者，他们对脆弱性的攻击可能就是更大的破坏力的前兆。

目前所观察到的几次攻击都没有特别明确的攻击目的，攻击能力也还没有完全体现出来，要了解威胁和脆弱性的长期趋势就必须加强网络威胁分析。到目前所知，攻击工具和攻击方法已经逐步扩散并比较容易获得，有意制造混乱和破坏的用户的技术能力和熟练程度正逐步提高。

在和平时期，美国的敌人可能对我们的政府、大学的研究中心和私营公司开展间谍活动，他们也可能预先摸清美国信息系统的情况、选择重要的目标并安装后门或其他访问渠道以袭击我们的基础设施。在战争或危机时期，敌人可能攻击关键基础设施和重要的经济功能，或打击公众对信息系统的信心，以达到恐吓国家政治领导人的目的。

对美国信息网络的攻击能够带来严重的后果，如导致关键运行中断、对财产和知识产权带来损失或导致人身伤亡。对于这些攻击，如果要降低脆弱性、遏制敌人对关键基础设施进行危害的能力和动机，就必须发展稳健的对抗能力，但这种能力目前我们还不具备。

### 政府在网络空间安全中的角色

一般而言，私营部门具有良好的技术装备和组织结构，最适合承担对不断变化的网络威胁做出响应的任务。但是也有例外，有时由联邦政府对网络威胁做出响应是最为合适和正当的。

从内部看，政府为维持自身的持续运作，就必须保护自身的网络基础设施和支撑其核心使命和服务的资源。从外部看，政府在网络安全工作上发挥的作用包括处理以下问题：事件的处理费用过高或者法律壁垒引发严重的协调问题；没有私营部门参与，必须政府处理的问题；对可能导致关键共享资源不足的紧急问题做出处理；提高公众网络安全意识。

公共-私营共同参与是保护网络空间战略的重要组成部分，原因在于以下方面：公共-私营合作有助于解决协调问题，可以明显增强信息交换和合作。公共-私营合作可以采用多种形式，其合作领域包括提高公众安全意识、培训、技术改进、脆弱性矫正以及对服务运营的恢复。

联邦政府机构对这一事务（或其他事务）中的角色是否合理取决于其行为带来的好处是否超过了相关的成本。当对任何可能的威胁或脆弱性有多个私营机构能够提供解决方案时，这一标准显得尤为重要。在所有情况下，政府采取每一行动时都必须广泛考虑该行动可能带来的成本和影响，应与其他可行方案以及不采取行动做比较，并考虑到私营机构当前或未来的解决方案。

法律授权联邦政府采取保护网络空间的行动以达到以下目的：司法取证和攻击源认定、保护国家安全中关键的网络和系统、迹象发现和预警、抵抗可能对经济造成危害的有组织的攻击。此外，联邦政府还必须支持研究和技术开发，使得私营部门能够更好地保护私有的国家关键基础设施。

### 国土安全部和网络空间安全

2002 年 10 月 25 日，布什总统签署了建立国土安全部的法令，这一新的内阁级部门将组织 22 个联邦机构共同保护我们的国土安全。国土安全部长将在保护网络空间上承担重要的职责，包括：

- 为保护美国的重要资源和关键基础设施制定一项全面的国家计划。
- 在关键信息系统受到威胁或攻击时开展危机管理工作。
- 向私营部门和其他政府实体对大规模关键信息系统故障的应急恢复计划提供支持。
- 与其他联邦机构协调，为州和地方政府、私营部门、其他实体和公众提供特定的预警信息以及适当的保护措施和对策。
- 与其他部门一起开展并赞助研发工作，为保护国土安全提供新的科学知识和技术。

与这些职责相应，国土安全部将成为联邦机构中的网络安全优秀中心，并为联邦政府向州、地方政府和非政府机构（包括私营部门、学术界和公众）的推广提供一个中心点。

### 保护网络空间安全的关键优先级

《保护网络空间的国家战略》清晰地描述了国家必须优先考虑的五项重要事务：

- I. 国家网络空间安全响应系统；
- II. 国家网络空间威胁和脆弱性消减计划；
- III. 国家网络空间安全意识和培训计划；
- IV. 保护政府部门的网络空间安全；
- V. 国家安全和国际网络空间安全合作。

第 I 项优先事务主要是改善对网络事件的响应，减少这些事件可能造成的破坏；第 II～IV 项优先事务的目标是减少网络攻击所可能带来的威胁，降低脆弱性；第 V 项优先事务的目标是防止破坏国家安全相关设施的网络攻击，改善国际对这些攻击的处理与响应。

### 优先事务 I：国家网络空间安全响应系统

攻击的快速标识、相关信息的交换和采取补救措施通常可以降低恶意网络行为带来的危害。对于全国性的攻击行为，美国需要在政府和私营企业之间建立合作联盟以分析攻击、发布预警并协调应急响应工作。在这个过程中必须保护隐私和公民自由。由于没有任何一个网络安全计划能够防止所有智能化、有组织的攻击，因此必须确保信息系统在受到攻击时仍能正常工作并可快速恢复所有功能。

《保护网络空间的国家战略》就网络空间安全响应确定了八项主要行动和工作：

- (1) 为响应国家级的网络安全事件，制定一个公共-私营合作的体系结构。
- (2) 为从战术和战略上分析网络攻击和评估脆弱性做好准备。
- (3) 鼓励私营部门加强把握网络安全总体态势的能力。
- (4) 扩展“网络预警和信息网”(CWIN)，支持国土安全部对网络安全危机管理的协调能力。
- (5) 改善对国家级事件的处理能力。
- (6) 在为公共-私营机构制定连续性计划和应急计划时，协调自愿参与的过程。
- (7) 对联邦政府的网络安全连续性计划进行演习。
- (8) 改善和加强公共-私营机构之间在网络攻击、威胁和脆弱性方面的信息共享。

### 优先事务 II：国家网络空间威胁和脆弱性消减计划

通过利用我们网络的脆弱性，有组织的攻击可能会对国家关键基础设施造成危害。关键基础设施的信息资产及其外部支撑结构（如 Internet 的运行机制）存在的脆弱性是对网络空间的最大威胁。脆弱性来源于技术的缺陷、不正确的技术实施方式和对技术产品缺乏了解。

《保护网络空间的国家战略》就消减网络威胁和脆弱性确定了八项主要行动和工作：

- (1) 增强司法机构防止和起诉网络攻击的能力。
- (2) 为国家网络脆弱性评估制定一个流程，以更好地把握网络威胁和脆弱性可能造成的后果。
- (3) 通过改进协议和路由方式增强 Internet 的安全性。
- (4) 鼓励使用可靠的数字控制系统（DCS）/监督控制和数据采集系统（SCADA）。
- (5) 减少和矫正软件的脆弱性。
- (6) 理解基础设施之间的互依赖性，改善网络系统和电信系统的物理安全。
- (7) 优先考虑国家网络安全研发工作。
- (8) 评估和加强新建系统的安全性。

### 优先事务 III：国家网络空间安全意识和培训计划

很多网络脆弱性之所以存在是由于部分计算机用户、系统管理员、技术开发人员、采购官员、审计人员、首席信息官（CIO）、首席执行官（CTO）和董事会缺乏网络安全意识。不论基础设施自身是否存在脆弱性，这种意识上的脆弱性将为关键基础设施带来很大的危险。由于缺乏足够受过训练的人员，网络安全行业也没有一个广泛承认的多级别的技能认证项目，这些都为处理网络脆弱性带来了困难。

《保护网络空间的国家战略》就安全意识、教育和培训确定了四项主要行动和工作：

- (1) 实施一项全面的国家级意识培养项目，使得包括商人、普通员工、一般民众在内的所有美国人都能够保护其自身所处的网络空间的安全。

- (2) 实施足够的培训和教育项目，以支持国家网络空间安全的需求。
- (3) 提高现有的联邦网络空间安全培训项目的效率。
- (4) 推动私营部门对得到良好协调的、广为认可的网络安全专业认证体系的支持。

#### 优先事务IV：保护政府网络空间的安全

虽然政府只管理着国家关键基础设施中的一小部分计算机系统，但各级政府在农业、食品、公共健康、应急服务、国防、社会福利、信息与通信、能源、运输、银行与金融、化学品、邮政和海运等领域承担着至关重要的任务，这些工作的执行都依赖于网络。在网络安全领域政府可以以身作则发挥领导作用，包括利用其采购计划培育网络安全产品市场。

《保护网络空间的国家战略》就保护政府的网络空间安全确定了五项主要行动和工作：

- (1) 不断对联邦政府的网络系统进行威胁和脆弱性评估。
- (2) 对联邦的网络系统用户实施身份鉴别和授权。
- (3) 保护联邦政府无线局域网的安全。
- (4) 改善政府外包和采购的安全性。
- (5) 鼓励州和地方政府考虑建设信息技术安全项目并与同类政府机构共享信息。

#### 优先事务V：国家安全和国际网络空间安全合作

美国的网络将美国和世界其他国家连接在了一起，一个覆盖全球的网络使得恶意攻击者可以对千里以外的系统实施攻击。网络攻击正以光速跨越国家边界，而且难以识别恶意活动的来源。美国必须能够保护自己的关键系统和网络的安全，为做到这点就需要有一个国际合作机制以便于交换信息、降低脆弱性和震慑恶意人员。

《保护网络空间的国家战略》就国家安全和国际网络空间安全合作确定了六项主要行动和工作：

- (1) 加强与网络相关的反情报工作。
- (2) 改善对攻击源调查和响应的能力。
- (3) 在网络攻击响应方面，加强对全国国家安全部门的协调。
- (4) 与工业界一起，通过国际组织，推动国际间的公共部门和私营部门就保护信息基础设施和促进全球的“安全文化”开展对话。
- (5) 促进建设全国性和国际性的观察和预警网络，以在网络攻击发生时及时发现并将其制止。
- (6) 鼓励其他国家加入《欧洲委员会计算机犯罪公约》，或至少确保这些国家的法律和流程中包含了该约定的内容。

#### 举国努力

保护广泛分布的网络资产的安全需要很多美国人的共同努力，联邦政府没有足够的能力单独保护美国的网络疆土，我们联邦制度的传统和有限的政府部门使得需要联邦政府以外的其他机构来领导其中的一些工作。政府鼓励任何能够为保护网络空间安全做出贡献的人在这方面做出努力。联邦政府邀请人们与其一起创建公私合作联盟，以提高网络安全意识、培训人员、刺激市场、改进技术、发现和矫正脆弱性、交换信息和制定运行恢复计划。

美国人民和各机构已经就改善网络空间的安全性做出了很多努力，2002年9月18日，很多私有实体发布了保护自身基础设施的计划和战略。关键基础设施安全合作组织（PCIS）在推

动私营实体协助制定本战略上发挥了不寻常的作用。关键基础设施部门提出的建议可以从<http://www.pcis.org> 上得到（这些文档并未经过政府的批准）。

这些基础设施计划描述了以下各部门的战略行动：

- 银行与金融；
- 保险；
- 石油和天然气；
- 电力；
- 执法机构；
- 高等教育部门；
- 运输（铁路）；
- 信息技术和通信；
- 供水。

一旦每个关键基础设施部门均实施了这些计划，我们的基础设施的威胁和脆弱性将会降低。

在可以预见的未来，以下两件事是毋庸置疑的，一是美国将继续依赖网络空间，二是联邦政府将寻求建立一个持续、广泛的合作联盟来制定、实施并改善本部战略。

## 2. 介绍

### 网络上的国家

国家的基础设施由多个行业的公共和私营机构的实物资产和网络资产构成。这些行业包括农业、食品、供水、公共健康、应急服务、运输、银行与金融、化学品和危险物质、邮政和航运。网络空间是这些基础设施的神经系统，是我们国家的控制系统。网络空间由成千上万个互联的计算机、服务器、路由器、交换机、光纤构成，它们是关键基础设施运作的基础。因此，网络空间的健康运行对经济建设和国家安全至关重要。不幸的是，最近很多事件表明网络空间确实存在着很多脆弱性，而且有恶意人员正试图利用这些脆弱性（参见后文“网络空间威胁和脆弱性”）。

《保护网络空间的国家战略》是保护国家的总体战略的一个要素，是《国土安全国家战略》具体实施的一个构成部分，《关键基础设施和重要资产的物理保护国家战略》是对这一战略的补充。本文的目的是使美国人能够保护其所拥有、运营、控制或互联的那一部分的网络空间。保护网络空间是一个艰巨的战略挑战，需要包括联邦政府、州和地方政府、私营部门及所有的美国人民在内的整个社会的共同努力。

### 独特的问题，独特的过程

多数关键基础设施以及他们所依赖的网络空间为私人所拥有和运营，私营机构和教育机构的创新使得创造和支撑网络空间的新技术不断发展。政府自身并无法单独保护网络空间的安全，因此布什总统呼吁政府、工业界、教育机构和非政府组织自愿联合起来共同保护网络空间的安全（参见后文“国家政策与指导原则”）。

考虑到这种合作联盟的重要性，制定《保护网络空间的国家战略》的一个环节就是充分听取来自公共机构和私营机构的观点。为此，白宫赞助了在十个大城市举行的关于网络安全市政

大会。接着，不同的部门（如高等教育部门、州政府和地方政府、银行与金融）分别组织工作组以制定了该部门具体的网络空间保护战略。另外，白宫还建立了一个总统顾问小组——国家基础设施咨询委员会（NIAC）。该委员会包括了来自经济、政府、教育等核心部门的领导。总统的国家安全电信咨询委员会（NSTAC）负责审查了本战略，并提出了修改意见。

2002年9月，总统关键基础设施保护委员（PCIPB）将本战略的草案在网上公开以听取来自全国所有个人和机构的意见。数千人参加市政会并提出了建议，他们的建议有助于确定本战略的最终内容，使得本战略的主题和提出的优先事务更有针对性。

这个过程证明只有调动整个国家的所有主要机构一起努力才能成功保障网络空间的安全。联邦政府设计了本战略的制定流程以提高所有人民对网络安全重要性的认识，其目的是使得很多美国人感到自己参与制定了这个战略并提出了建议。

虽然修改后的草案反映了很多人提出的建议，但不是每个人都完全同意本战略中的每一部分。有些内容不能在本战略中详细阐述，有些观点的成熟度还不够，不足以成为一个国家政策。本战略并不是一成不变的，技术的进步、威胁和脆弱性的改变、对网络空间安全问题更为清晰的理解都使得我们有必要采取进一步的行动，因此还必须就网络空间安全问题继续举行全国性的对话。

在本战略的草案版发布后数周，国会通过了建立国土安全部（DHS）的议案，DHS包含了从事网络安全工作的很多机构，并将指引这些机构执行新的网络安全使命，本部战略反映了这些变化。议会已经通过《网络安全研究和开发法》（公法 107-305），并由总统签署生效。该法授权政府花若干年时间的努力来开发更为安全的网络技术、扩大网络安全研究和开发工作、改善网络安全人力资源。

### 五项与国家网络空间安全相关的优先事务

《保护网络空间的国家战略》号召全美国的所有个人和机构提高意识并采取行动，以提高全国的网络安全级别，不断发现和矫正网络脆弱性。本战略的基本框架是对五项优先事务的日程安排，这些事务需要广泛的自愿性参与。每个行动项目均包含几个组成部分，其中很多部分来自本战略草案版的建议以及公众的评论。

这些优先事务的处理既需要国土安全部的领导，也需要其他几个重要的联邦部门的参与。其预算由管理和预算办公室（OMB）负责，在国会的支持下，这些部门现在都有责任将本战略提出的建议付诸行动。

同时，也鼓励公司、高校、州政府、地方政府以及其他合作伙伴开展与这五项优先事务目标一致的行动，这些行动可以是独立行动，也可以与联邦政府合作。每个私营部门都必须在成本有效性分析、风险管理及危机减缓战略的基础上自主做出决定。

《保护网络空间的国家战略》清晰地描述了国家将优先考虑的五项重要事务，第Ⅰ项优先事务主要是改善对网络空间事件的响应以及减少这些事件可能造成的破坏。第Ⅱ～Ⅳ项优先事务的目标是降低网络攻击所可能带来的威胁，消灭我们的脆弱性。第Ⅴ项优先事务的目标是防止发生可能对国家资产造成破坏的网络攻击，改善国际间对这些攻击的响应与合作。

#### （1）优先事务Ⅰ：国家网络空间安全响应系统

攻击的快速识别、相关信息的交换和采取补救措施通常可以降低恶意网络行为带来的危害。对于全国性的攻击行为，美国需要在政府和私营企业之间建立合作联盟以分析攻击、发布



预警并协调应急响应工作。在这个过程中必须保护隐私和公民自由。由于没有任何一个网络安全计划能够防止所有智能化的有组织的攻击，因此必须确保信息系统在受到攻击时仍能够正常工作并能够快速恢复所有功能。为对可能发生的大型攻击做好准备，美国需要一个国家级网络灾难恢复计划，国家网络空间安全响应系统将公共-私营机构以及网络中心一起实施分析、监测和预警工作，并加强信息交换，推动恢复工作。

#### （2）优先事务II：国家网络空间安全威胁和脆弱性消减计划

通过利用网络的脆弱性，有组织的攻击可能会对国家关键基础设施造成危害。关键基础设施的信息资产及其外部支撑结构（如 Internet 的运行机制）存在的脆弱性是对网络空间的最大威胁。脆弱性来源于技术的缺陷、不正确地实施方式和对技术产品缺乏了解。

国家网络威胁和脆弱性消减计划将在全国范围内协调政府和私营部门共同合作，如共享最佳实践措施、共同评估和实施新技术，以发现和矫正最严重的网络脆弱性。本项事务的其他构成部分包括提高网络安全意识、增加犯罪司法调查活动、制定对未来可能出现的网络威胁起到震慑作用的国家级安全项目。

#### （3）优先事务III：国家网络空间安全意识和培训计划

很多网络脆弱性之所以存在是由于部分计算机用户、系统管理员、技术开发人员、采购官员、审计人员、首席信息官（CIO）、首席执行官（CTO）和董事会缺乏网络安全意识。不论基础设施自身是否存在脆弱性，这种意识上的脆弱性为关键基础设施会带来很大的危险。缺乏足够受过训练的人员，网络安全行业也没有一个广泛承认的多级别的技能认证项目，这些都为处理网络脆弱性带来了困难。

国家网络安全意识和培训项目将提高公司、政府部门、大学和全国的计算机用户的网络安全意识，它还将解决缺乏受过训练和通过认证的网络安全工作人员的问题。

#### （4）优先事务IV：保护政府网络空间的安全

虽然政府只管理着国家关键基础设施中的一小部分计算机系统，但各级政府在农业、食品、公共健康、应急服务、国防、社会福利、信息与通信、能源、运输、银行与金融、化学品、邮政和海运等领域承担着至关重要的任务，这些工作的执行都依赖于网络。在网络安全领域政府可以以身作则发挥领导作用，包括利用其采购计划培育网络安全产品市场。部署这些产品将有助于保障联邦政府的计算机系统和网络的安全。

#### （5）优先事务V：国家安全和国际网络安全合作

美国的网络将美国和世界其他国家连接在一起，一个覆盖全球的网络使得恶意攻击者可以对千里以外的系统实施攻击。网络攻击正以光速跨越国家边界，而且难以标识恶意活动的来源。美国必须能够保护自己的关键系统和网络的安全，为做到这点就需要有一个国际合作机制，以便于交换信息、降低脆弱性并震慑恶意人员。

### 行动和建议

本战略强调联邦政府将听取非政府机构中的合作伙伴的建议并向其提出建议。在本战略中具体的行动和建议（A/R）以斜体标识，并依照其相关的优先事务编排号码。例如，A/R 1-1 是优先事务 I 中的第一个行动或建议。附录 A 提供了所有 A/R 的概要。

### 3. 网络空间威胁和脆弱性

#### 行动案例

恐怖分子在 2001 年 9 月 11 日对美国实施了攻击，这对我们的国家有着深远的影响。整个联邦政府和社会被迫重新检讨对国土安全的认识，很多人第一次意识到我们国家的敌人将造成的破坏可能达到什么样的程度。

我们必须进一步认识到有很多敌人试图破坏我们的生活方式，他们准备攻击我们的本土，并倾向于使用非正规方法实施攻击。“9·11”的攻击是现实的物理性攻击，而我们在网络王国中也同样面临着日渐增加的来自敌人的威胁。

#### 完全依赖于网络空间的国家

对于美国来说，信息技术革命正悄悄地改变着商业和政府的运作方式。在没有充分考虑安全性的情况下，国家将制造业、公共事业、银行和通信的核心操作交给计算机网络控制，这使得交易成本得到了降低而生产力急速提升。人们越发使用联网系统的趋势还在继续，到了 2003 年，我们的经济和国家安全已经完全依赖于信息技术和信息基础设施。由多个网络互联构成的大规模网络直接支撑着我们的所有经济部门的运作，包括能源（电力、石油、天然气）、运输（铁路、航空、船运）、金融和银行、信息与通信、公共健康、应急服务、供水、化学品、国防工业基础、食品、农业、邮政和海运。计算机网络的触角超越了网络空间的范围，它们还控制着像变压器、火车、输油管、油泵和雷达等物理设备。

#### 网络空间中的威胁

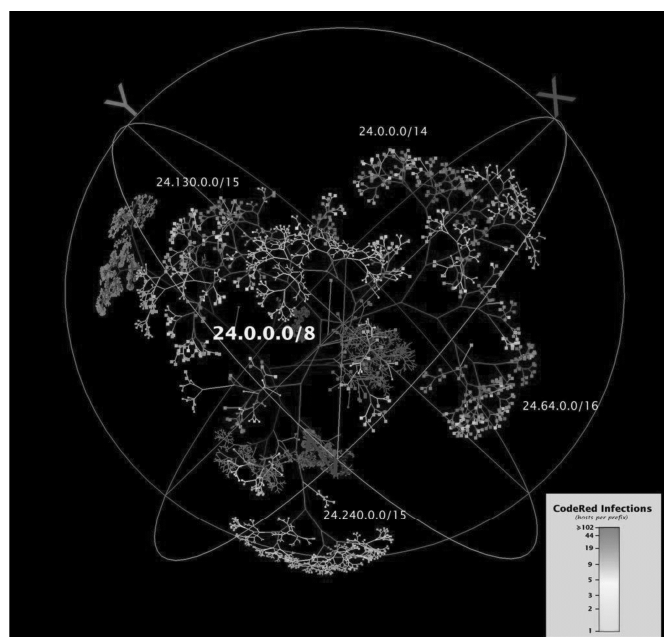
一些恶意人员能够对我们的关键信息基础设施实施攻击，最受关注的是有组织的网络攻击能够破坏国家关键基础设施、经济建设并危害国家安全。实施这种攻击要求具有高超的技术，这从一定程度上解释了为什么到目前为止还很少出现这种攻击。但是我们不能太过乐观，当前已经有一些有组织的攻击者，他们对脆弱性的攻击可能就是更大的破坏力的前兆。

目前所观察到的几次攻击都没有特别明确的攻击目的，攻击能力也还没有完全体现出来，要了解威胁和脆弱性的长期趋势就必须加强网络威胁分析。到目前所知，攻击工具和攻击方法已经逐步扩散并比较容易获得，有意制造混乱和破坏的用户的技术能力和熟练程度正逐步提高。

例如，就“NIMDA”（尼姆达，“ADMIN”的倒序拼写）攻击而言，虽然事实上它并没对关键基础设施造成灾难性的破坏，但它表明网络攻击技术的成熟程度正逐步提高，还表明有组织的攻击者已经具有较强的学习能力并已经习惯在网络环境下工作。“尼姆达”是一种自动化网络攻击，是一种计算机蠕虫和计算机病毒的混合体。它以很快的速度在全国传播，尝试采用多种不同的方法感染其入侵的计算机系统，直到获得控制权并破坏文件。它在 1 小时内从一个未知的地方传遍全国并攻击了 86 000 台计算机，这次攻击持续了数天。

网络攻击的速度也在逐步提高，在“尼姆达”出现前两个月，一个名为“红色代码”的蠕虫在 14 小时内感染了 150 000 台计算机，此后出现的“尼姆达”的传播速度比“红色代码”的传播速度要高得多。

“红色代码”在 Internet 上的渗透如下图所示：



由于计算机攻击工具日益成熟，有能力对我们的基础设施和网络空间实施攻击的人数也正在增加。在和平时期，美国的敌人可能对我们的政府、大学的研究中心和私营公司开展间谍活动，他们也可能预先摸清美国信息系统的情况，选择重要的目标并安装后门或其他访问渠道以袭击我们的基础设施。在战争或危机时期，敌人可能攻击关键基础设施和重要的经济功能，或打击公众对信息系统的信心，以达到恐吓国家政治领导人的目的。

对美国信息网络的攻击能够带来严重的后果，如导致关键运行中断、对财产和知识产权带来损失或导致人身伤亡。对于这些攻击，如果要降低脆弱性、遏制敌人对关键基础设施进行危害的能力和动机，就必须发展稳健的对抗能力，但这种能力目前我们还不具备。

网络空间为攻击者提供了一个攻击渠道，使其能够从远处对我们的基础设施实施有组织的攻击。这些攻击只需要常用的技术，攻击者能够隐藏其身份、地点和攻击的路径。网络空间不仅使别人能够利用脆弱性攻击我们的关键基础设施，而且也加剧物理攻击提供了一个杠杆，包括可能中断通信、阻碍美国在防御或进攻上的响应、延缓应急响应（发生物理攻击之后应急响应变得非常重要）。

在 20 个世纪，物理上的隔离使得美国免于受到直接入侵，但在网络空间中国界并没有太大意义，信息在不同的政体、民族和宗教之间自由流动。甚至连构成网络空间的基础设施（硬件和软件）的设计和开发过程也是全球化的。由于网络空间全球化的特点，存在的脆弱性也是对整个世界上开放的，任何人在任何地方都能够利用这些脆弱性。

#### 在未知的威胁面前减少网络的脆弱性

在国家关键基础设施的威胁增加时当然必须要做出相应的处理，但是，如果在发生攻击之前不重视研究关键基础设施的脆弱性，而只是被动等待攻击，显然是危险且不可取的。通过网络攻击可能突袭国家的网络，预先没有任何征兆并且快速传播，很多受攻击的对象在此之前根本来不及得到预警信息。即使预先得到警告信息，也可能没有足够的时间、知识或必备的工具来保护自己。有时找到对抗攻击的方法可能就需要很长时间。

从很多网络攻击得到的经验教训是，对网络系统具有依赖性的机构必须采取积极措施，预先发现并矫正其网络的脆弱性，而不是在得到攻击预警或受到攻击时才采取行动。现在就必须进行脆弱性评估并矫正脆弱性，由受过训练的专业人员实施信息技术安全审计以标识基础设施的脆弱性，这个过程可能需要几个月的时间。接着可能还需再花几个月的时间制定多层次的防护措施、创建自恢复能力较强的网络以矫正最为严重的脆弱性，这一过程还必须定期重复实施。

### **威胁和脆弱性：5个级别上的问题**

由于网络空间用户的数量巨大且类型各异，处理威胁和降低脆弱性是一个相当复杂的问题。事实上，无数设备通过很多网络互联，保护网络的安全需要由不同的人在多个级别采取行动，可以在5个不同的级别上解决网络空间的安全问题。

#### **第1级：家庭用户/小型商业机构**

虽然家庭用户的计算机不是关键基础设施的一部分，但是这些计算机可能被远程控制并用于对关键基础设施实施攻击。毫无防护的家庭用户或小商业机构的计算机，特别是DSL或宽带用户容易受到攻击。攻击者可以在计算机主人毫无知觉的情况下利用这些计算机。其他人可以用一组这样的“僵尸”对关键网络节点或其他重要企业或关键基础设施实施拒绝服务攻击。

#### **第2级：大型机构**

大型机构（公司、政府机构和大学）经常是网络攻击者的目标，很多这些大型单位是关键基础设施的一部分。这些机构需要有效的、清晰明确的信息安全政策和计划，确保其用户遵循了安全规范。根据美国情报部门的说法，恶意人员将会增加对美国的网络的攻击，既为了从这些获取数据，也为了利用这些网络。

#### **第3级：关键部门/关键基础设施**

经济部门、政府部门和学校团体可以联合起来解决常见的网络安全问题，比起单独解决问题来说，这样通常可以降低各个单位的负担。这种合作将导致他们依赖相同的机构和机制，这反过来使得有些脆弱性一旦被利用，就可能破坏所有的成员部门的正常运作。各个部门还可以通过参加各种小组以降低风险，这些小组将研究最佳解决方法、评估技术方案、评测产品和服务并交换信息。

有几个部门已经建设了自己的信息共享和分析中心（ISAC）以监测对其各自的基础设施的网络攻击。ISAC同时还是共享攻击动态、脆弱性和最佳实践措施的信息通道。

#### **第4级：国家事务和全国性脆弱性**

有些网络安全问题是全国性的问题，企业或基础设施部门无法单独解决这种问题。所有部门使用的是同一个Internet，如果Internet的机制不安全将会危及所有部门。广泛使用的软硬件中存在的脆弱性也可能导致全国性的问题，这便需要全国协同努力来研究开发出改良的技术。另外，国家缺乏受过培训和通过认证的网络安全专业人员，这一问题值得引起整个国家的关注。

#### **第5级：全球**

全世界的网络是由全球性的信息系统构成的，相同的标准使得全世界的计算机系统能够互

操作。但是，这种互联也意味着在世界一端的计算机出现的问题有可能会对世界另一端的计算机造成影响。因此，我们依赖于国际合作，以共享与网络事件相关的信息并进一步起诉网络犯罪。如果没有这种合作，我们发现、震慑和减少网络攻击的能力将大大降低。

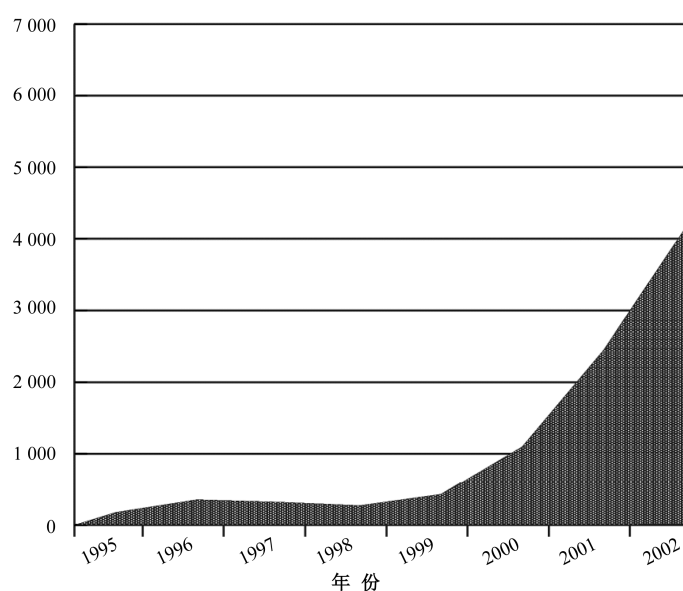
网络空间中各方的角色和职责见下表：

	优先事务 I	优先事务 II	优先事务 III	优先事务 IV	优先事务 V
	国家网络空间安全响应系统	国家网络空间安全威胁和脆弱性消减系统	国家网络空间安全意识和培训计划	保护政府网络空间的安全	国家安全和国际网络空间安全合作
家庭用户/小型商业机构		✕	✕		
大型机构	✕	✕	✕	✕	✕
关键部门/基础设施	✕	✕	✕	✕	✕
国家事务和全国性脆弱性	✕	✕	✕	✕	
全球					✕

### 新的脆弱性需要持续的响应

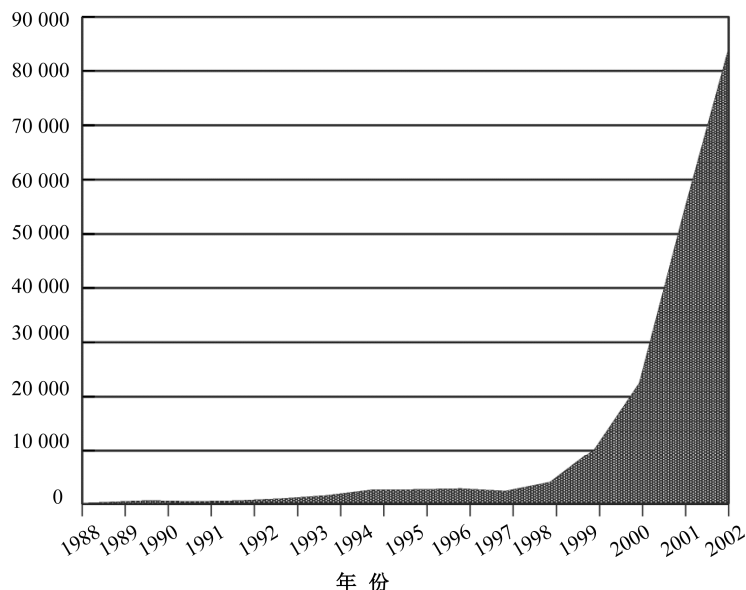
人们总是不断发现或制造新的脆弱性，因此保护网络和系统的过程是不可中断的。计算机应急响应小组/协调中心（CERT/CC）注意到，不仅网络事故和攻击以惊人的速度增加，攻击者可以利用的脆弱性也在以很高的速度增长。计算机安全脆弱性（即软件或硬件中存在的错误，它们可用于非授权访问系统或破坏网络）从 2000 年到 2002 年明显增加，脆弱性的数目已从 1 090 个增加到 4 129 个。

CERT-CC 报告的脆弱性数目（1995—2002 年）如下图所示：



只安装网络安全设备并不能取代对网络的经常性维护。最近计算机安全学会（CSI）的一次调查表明，在被调查的人员中，85%使用了反病毒软件。在同一调查中，89%的人员安装了计算机防火墙，60%的人员安装了入侵检测系统。但是，90%的人报告曾经受到攻击，40%的系统曾经被网络外部的人员入侵。

CERT-CC 报告的事件数目（1998—2002 年）如下图所示：



通过采取较好的安全措施可以消除绝大多数的脆弱性。但是，以上调查说明，好的安全措施并不仅仅是安装这些软件或硬件，还要求人们正确地使用它们，并需要经常打补丁或升级病毒库以确保这些防护措施是最新的。

### 网络安全及其机会成本

对于每个公司和整个国家来说，提高计算机安全都需要投入精力、时间和金钱。在 2003 财政年度，布什总统要求国会为保护计算机安全增加 64% 的预算。布什总统现在对计算机网络安全上的投入的这些预算将会降低国家整体的开销，通过电子政务、现代企业管理、减少浪费和欺诈等措施将能够节省开支。

对于整个国家的经济，特别是对于信息技术产业，缺乏可信、可靠、安全的信息系统将阻碍未来经济的增长。信息技术革命还可能以多种途径加速经济增长，但是这些增长途径的实现要受到网络安全问题的制约。网络空间的脆弱性不仅会危及网络交易，还危及知识产权、商业运行、基础设施服务和消费者的信心。

网络安全投资不会只是昂贵的日常性开支，这种投资是会有所回报的。有关调查已不断表明：

- 虽然遭受严重网络攻击的可能性很难估计，但一次成功的攻击带来的损失可能要大于实施计算机安全项目的开销。
- 在一个机构的信息系统体系结构中设计强安全协议可以降低整个运营成本，因为这些安全协议可以使很多用来节省成本的措施得以实现，如远程访问、顾客或供应链的互

动等。在没有安全网络的情况下，这些措施都是无法实现的。

这些结果表明，公司的网络安全意识越强，就越能够从其网络安全中获益。增强意识和自愿参与是《保护网络空间的国家战略》中的一个重要组成部分。

### 个人与国家的风险管理

截至 2001 年 9 月 11 日之前，跨国恐怖组织对美国造成的破坏并不大，而到了这一天，一切很快发生了改变。有人估计，对美国信息系统的攻击造成的损失在过去 4 年内增长了 4 倍，虽然这些损失相对来说并不显著，但是它们可能会突然迅速增加。

网络攻击每天都威胁着美国的各个公司和家庭计算机用户，这些攻击造成了一定程度的破坏，并给受害者带来了很大的损失。它们可能导致全国性的破坏并给国家带来损失，还可能影响到国家所依赖的网络和系统。以下是导致这些攻击的原因：

- 敌人有攻击的意图；
- 用于实施攻击的工具唾手可得；
- 国家的信息系统存在很多众所周知的脆弱性。

没有一种策略能够彻底消除网络空间的脆弱性及其相关的威胁。不论怎样，国家必须行动起来担负起风险管理的责任，提高管理能力以减少攻击带来的损失。1997 年总统委员会在一份公开的报告中指出了这种风险；2000 年发布了第一份针对该问题的国家计划，2001 年布什总统在一份行政命令中提到了这些风险并将网络安全作为一项优先事务来抓，并相应地增加了保护联邦网络的资金；2002 年，总统在提议成立国土安全部时也建议将巩固和加强联邦网络安全作为国土安全部的一项职责。

### 政府无法单独保护网络空间安全

虽然公众对网络安全的重要性的意识已经有所提高，而且已经采取的一些措施增强了我们的能力，但是我们国家的信息网络及其管理下的关键系统中仍然潜藏着网络风险。降低网络风险要求在国家的不同部门以及在国际之间建立一种空前广泛的合作关系。

联邦政府不能（事实上也不应该）保护私有的银行、能源公司、运输公司和其他私营实体的计算机网络。联邦政府同样也不能到家庭、小型单位、学校、州政府或地方政府去建设安全的计算机网络。每个依赖于网络空间的美国人都必须保护他们拥有或负责的那部分网络空间的安全。

## 4. 国家政策与指导原则

### 国家政策、原则和组织

本节描述《保护网络空间的国家战略》所依据的国家政策以及相应的基本框架。同时还描述了联邦政府在其中扮演的角色和承担的职责。

### 国家政策

信息技术革命改变了商业交易模式、政府的运行方式和国防建设模式。这三者目前都依赖于由关键信息基础设施组成的互依赖网络，我们称其为“网络空间”。

防止或尽量减少关键信息基础设施服务的中断，以保护人民、经济、重要的公民和政府服

务以及国家安全，是美国的一项基本政策。必须减少服务中断发生的次数和持续时间，使其可控并尽可能减少损失。这一政策要求我们不断努力保护关键基础设施中信息系统的安全，并需要结成自愿的公共-私营合作联盟，企业 and 非政府组织将参与其中。

与《国土安全国家战略》相一致，《保护网络空间的国家战略》的目标是：

- 防止对美国关键基础设施的网络攻击；
- 减少国家对网络攻击的脆弱性；
- 在出现网络攻击时，尽量减少损失并缩短恢复时间。

### 指导原则

2001 年 1 月，本届政府开始研究信息系统和网络安全的重要性。2001 年 10 月，布什总统签署了 13231 号行政令，授权成立一项旨在通过不断努力来保护关键基础设施中的信息系统的保护项目，包括对应急战备通信设施及其相关的物理设施进行保护。《联邦信息安全管理法》（FISMA）和 13231 号行政令以及其他相关的总统令和法规条令共同构成了保护网络空间安全的行政框架。

保护这些信息系统对于每个经济部门都是至关重要的，实施这一保护计划，必须依循以下的组织原则。

（1）举国努力：保护网络空间的广泛分布的设施需要所有美国人的共同努力，联邦政府无法单独保护美国人的网络空间。联邦制的传统和有限的政府部门使得需要联邦政府以外的其他机构来领导其中的很多工作。政府部门在保护网络空间方面发挥的作用还包括保护私营基础设施的安全，包括：

- 召集并推动政府和非政府实体间的讨论；
- 确定何种情况下普通人遇到的常规安全事件会影响到国土、国家和经济安全；
- 与非政府实体共享网络空间威胁和脆弱性方面的信息，使其能合理地调整风险管理战略和计划。

在任何情况下，政府都只有在其对私营部门的干预所带来的好处超过其行为的直接和非直接代价时才实施干预行为。

政府鼓励每个美国人参与保护网络空间的安全，联邦政府将致力于促进创建和参与公共-私营合作联盟，以提高安全意识、培训人员、刺激市场、改进技术、发现和矫正脆弱性、交换信息以及对系统正常运营的恢复做出规划。很多部门在创建信息共享和分析中心（ISAC）方面发挥了重要的作用，它们促进了交流、开发了最佳的实践措施，并发布了与网络安全相关的信息。另外，有几个部门还制定了保护自身网络空间的计划，它们是本战略的补充，政府期望这种有效的合作联盟能得以继续。

（2）保护隐私和公民自由：滥用网络会侵犯我们的隐私和自由，联邦政府有责任避免网络的滥用和公民自由遭到侵犯。网络安全和个人隐私并不矛盾，网络空间安全项目必须增强而不是降低对个人隐私的保护，因此，必须注意尊重个人隐私和公民自由。消费者和运营商必须就其共享的秘密信息达成共识，对私人信息必须准确地、秘密地、可靠地实施处理。联邦政府将在保护隐私方面起示范作用并付诸行动。作为这一过程的一部分，联邦政府将定期咨询隐私倡导者和相关专家的意见。

（3）规章制度与市场作用：在保护网络空间方面，联邦政府的规章制度将不会发挥主要作



用。如果通过规章制度规定每个公司必须如何配置其信息系统，这等于选择了一个固定的安全高度，也就排斥了更好的安全解决方案，这种安全措施会被快速发展的新技术所淘汰。甚至更糟糕的是，这种措施会导致比现有网络更不安全和更为同构的网络系统。在法律方面，联邦的法规部门已经开始考虑通过法律手段保护网络安全。然而，人们还是期望市场自身能够为增强网络安全提供最主要的动力。

(4) 职责：《保护网络空间的国家战略》的主要目标是建设更具有抗攻击能力的、可靠的信息基础设施。它规定了负责联邦网络空间保护工作的领导部门和机构。2002 年 12 月 25 日，总统签署了 2002 年《国土安全法》，建立了国土安全部。国土安全部承担了本战略中制定的很多项目。本战略还向联邦政府、州和地方政府、私营机构及美国人民就如何保护网络空间提出了建议。

(5) 确保灵活性：网络威胁变化很快，因此，应强调对网络攻击做出响应和减少脆弱性的能力必须具有灵活性。攻击工具的迅速发展为攻击者提供了便利，它们可以迅速修改攻击策略，针对网络信息系统和管理机构的响应能力的弱点实施攻击。灵活的计划使得各个部门能够在网络威胁发生变化时重新评估各项工作的重要程度并重新调整资源。

(6) 为期多年的计划：保护网络空间的工作正在向前推进，这一过程中还会出现新的技术并发现新的脆弱性，本战略为保护网络空间安全提供了一个初步框架，各个部门必须根据自身的角色，采纳为期多年的网络安全计划，同时也鼓励其他公共或私营组织这样做。

### 国土安全部与网络空间安全

国土安全部由 22 个联邦实体所联合成立，这 22 个联邦实体的共同目标是改善国土安全。在处理可能影响联邦政府甚至整个国家网络基础设施的安全事件上，国土安全部将发挥核心作用。国土安全部长将在网络安全方面承担重要的职责，包括：

- 制定一项全面的国家计划，以保护美国的重要资源和关键基础设施，包括信息技术和电信系统（包括卫星）以及支撑这些系统的物理资产和技术资产。
- 在关键信息系统受到威胁或攻击时开展危机管理工作。
- 向私营部门和其他政府实体对大规模关键信息系统故障的应急恢复计划提供支持。
- 与其他联邦机构协调，为州和地方政府、私营部门、其他实体和公众提供特定的预警信息以及适当的保护措施和对策。
- 与其他部门一起开展并赞助研发工作，为保护国土安全提供新的科学知识和技术。

### 协调机构

联邦政府和私营部门之间的有效合作依赖于高效的协调和交流。为促进和加强这种合作结构，政府为基础设施可能受攻击的主要经济部门指定了“领导机构”。另外，科技政策办公室（OSTP）负责协调关键基础设施保护方面的科研工作。管理和预算办公室（OMB）负责监督联邦政府的计算机安全项目中的政策、原则、标准和方针在整个政府部门的实施情况。美国国务院负责协调网络安全方面的国际协作事务。中央情报局负责评估其他国家对美国的网络和信息系统的威胁。司法部和联邦调查局负责对网络犯罪的调查和起诉工作。

关键基础设施领导机构见下表：

领导机构	关键基础设施部门
国土安全部	<ul style="list-style-type: none"> <li>➤ 信息与通信；</li> <li>➤ 运输（航空、公共运输、水运、天然气管道、高速公路）；</li> <li>➤ 邮政和海运；</li> <li>➤ 应急服务；</li> <li>➤ 政府持续性</li> </ul>
财政部	<ul style="list-style-type: none"> <li>➤ 银行与金融</li> </ul>
健康和公众服务部	<ul style="list-style-type: none"> <li>➤ 公共健康（包括预防、监视、化验室和个人健康服务）；</li> <li>➤ 食品（不包括肉类和禽类食品）</li> </ul>
能源部	<ul style="list-style-type: none"> <li>➤ 供水；</li> <li>➤ 化学工业和危险物品管理</li> </ul>
农业部	<ul style="list-style-type: none"> <li>➤ 农业；</li> <li>➤ 食品（肉类和禽类食品）</li> </ul>
国防部	<ul style="list-style-type: none"> <li>➤ 国防工业基地</li> </ul>

政府将继续支持发展公共-私营合作联盟，行业的代表将和联邦的领导机构一起评估其在网络攻击和物理攻击方面的脆弱性，并对如何消除重大的威胁提出计划和对策。技术环境和威胁环境都可能很快发生变化，因此，各个部门和领导机构都必须经常评估国家基础设施的可靠性、脆弱性和威胁的环境，并采取适当的保护措施。

政府的所有权力、能力以及资源都可以用于支持基础设施的保护工作，包括危机管理、执法、规章制度的实施、境外情报和国防战备。

## 5. 优先事务 1：国家网络空间安全响应系统

在 20 世纪 50 年代和 60 年代，导弹和飞机带来的威胁使我们的国家第一次显得易受攻击。联邦政府对此做出了响应，创建了一个国家级系统，实现：使用雷达检测领空以发现异常行为；对可能出现的攻击进行分析并预警；在受到攻击时调动战斗机实施保护；在受到攻击后通过民防项目重建国家。

现在，国家的关键资产可能受到来自网络的攻击，美国需要一个不同的国家响应系统以发现网络空间中可能出现的破坏行为，分析脆弱性并向可能受攻击的对象发出警告，还应协调应急响应工作，恢复受到破坏的关键服务。

网络空间的主要部分并非由单一的公共或私营部门所拥有或运营，这对创建一个国家网络空间安全响应系统是一项挑战。对于网络空间无法画出一个全图或概要图，没有任何一个点可以集中判断攻击的来源或传播方向。虽然通过综合不同的组织提供的信息可以发现攻击（蠕虫、病毒、拒绝服务攻击），但是我们缺乏一个有组织的机制对这些信息做出分析并判断其含义。

### 国家网络空间安全响应系统

国家网络空间安全响应系统是一个在国土安全部领导和协调下的公私协作框架，其作用包括分析与警告、处理国家重大事件、保证政府系统和私营基础设施的持续可用、加强各个机构之间的信息共享以改善网络空间安全。国家网络空间安全响应系统包括政府实体和非政府实体，如私营部门的信息共享和分析中心（ISAC）。

为减轻网络攻击的影响，必须迅速广泛地传播关于攻击的相关信息。通过调动众多机构现有的分析能力和应急响应能力，便能够判断出抵抗攻击、减轻影响和恢复服务的最佳方法。

为国家网络空间安全响应系统建设一个合理的管理机制是另一项挑战。与冷战期间美国的领空监视计划不同，网络空间保护系统的操作人员往往不是联邦政府的雇员。因此，国家网络空间安全响应系统必须在政府和非政府部门合作的基础上实施。

国土安全部负责建设国家网络空间安全响应系统，这包括：

- 在关键信息系统受到攻击或威胁时做出响应，实施危机管理。
- 与其他联邦机构协调，为州政府和地方政府部门、私营机构、其他实体和公众提供特定的预警信息以及适当的保护措施和对策。

国土安全部将领导并协调国家网络空间安全响应系统方面的工作，这是其整个信息共享和危机协调工作的一部分，但是这个系统将包括来自政府和私营部门的很多组织。批准成立国土安全部的相关法律还要求设立一位处理隐私事务的官员，以确保与国家网络空间安全响应系统相关的任何机制在正确实施的同时能够保护公民的自由和隐私。这个官员将定期与隐私权提倡者、业界专家和公众讨论隐私方面的问题，以确保既能增强安全性又可保护隐私。

下面描述的是现有的联邦项目以及等待预算审核的新计划，还包括建议我们的合作伙伴实施的计划。

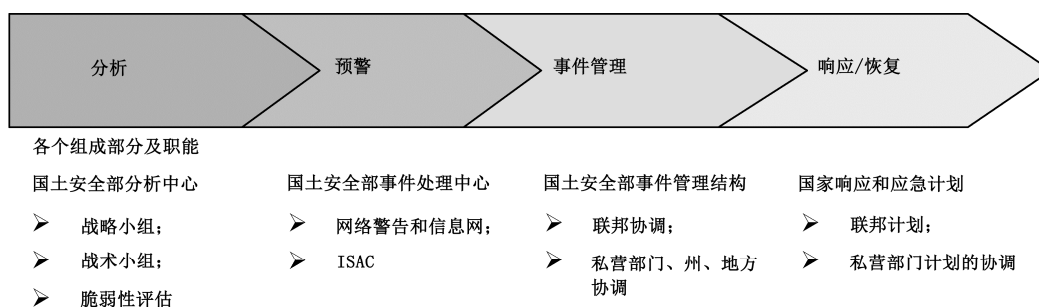
#### A. 为响应国家级网络事件而建立公私合作体系结构

并不需要为国家网络空间安全响应系统的建设专门制定一个代价昂贵的、官僚式的联邦项目。在很多情况下，这一系统将增强当前负责保护网络的几个重要的联邦机构的能力，它们现在已经是国土安全部的一部分。整合国家通信系统（NCS）、国家基础设施保护中心（NIPC）、联邦计算机事件响应中心（FCIRC）、能源保障办公室和关键基础设施保障办公室（CIAO）的资源将有助于为国家网络空间安全响应系统奠定必备基础。

私营网络受到的攻击越来越多，因此这些机构更有机会首先发现可能造成全国性影响的攻击。所以，各个信息共享和分析中心（ISAC）将在国家网络空间响应系统和整个国土安全的任务中发挥更加重要的作用。各个行业的 ISAC 对他们行业的核心工作有着独特的、深入的了解，其分析结果将有助于国家的工作。

信息共享和分析中心由业界领导，负责收集、分析、提炼、分解与特定部门相关的安全信息，并在此过程中发现并公布其最佳解决方法。信息共享和分析中心由多个部门共同设计，以满足其各自的需求并共同承担运营经费。国土安全部将与各个信息共享和分析中心紧密合作，确保他们能够即时得到与攻击和脆弱性相关的数据。

网络空间安全响应系统如下图所示：



### (1) 分析

#### a. 为从战术上和战略上分析网络攻击及脆弱性评估做准备

分析是深入了解网络事件及攻击的第一步，包括攻击的本质、泄漏的信息以及造成破坏的规模。分析还可以提供与攻击者的意图、使用的工具、利用的脆弱性相关的线索。对网络空间的分析有以下三种，这三种分析密切相关但并不相同。

(i) 战术分析：将通过分析网络事件相关的事实，找出脆弱性并提出预警。战术分析的例子包括：分析计算机病毒的传播原理以及及时找到保护或减轻破坏的方法；研究一次特定的计算机入侵事件或一组入侵事件以判断攻击者的意图和攻击方法。

(ii) 战略分析：不是分析特定的事件，而是更广泛地研究大量的事件及其背后的含义，判断事件对整个国家可能造成的影响。例如，战略分析可能分析威胁和脆弱性的长期发展趋势，并据此就新的攻击方法等正在增加的攻击发出预警。战略分析同时还为政策制定人员提供了信息，使其能够对未来的攻击进行预测并做好准备，由此可以减少攻击造成的破坏。战略分析还为确定迹象发现和预警的模式奠定了基础。

(iii) 脆弱性评估：是指对网络空间及其物理设施进行详细的检查以发现并研究其弱点。脆弱性评估是网络空间安全知识链中的一环，这些评估使得规划人员能够预测经济部门或政府部门的特定设施可能遭受的攻击后果。这些知识使得基础设施所有者和运营者能够增强其对各种威胁的抵抗能力（在网络空间安全威胁和脆弱性消减计划中将进一步讨论该问题）。

国土安全部将敦促各个领域增强分析能力。为此，它必须寻求包括信息共享和分析中心（ISAC）在内的私营部门的合作和支持。

### (2) 预警

#### a. 鼓励私营部门共享网络安全宏观信息

对 Internet 缺乏一个宏观的把握将阻碍人们提高分析 Internet 威胁、做出迹象发现或预警的能力。对一个部门的网络攻击可能扩大到其他很多部门并造成严重的后果，很多私营公司、州政府和地方政府可能没有能力处理这种情况。国土安全部组合了几个重要的联邦网络安全处理中心，形成了联邦政府处理自身网络安全紧急事务的核心机构，在必要的情况下，这一机构还可协助解决非联邦基础设施系统的网络安全问题。

政府鼓励工业界形成一种交换 Internet 安全综合信息的机制，以促进分析、预警、响应和恢复。在法律允许的范围内，非政府组织之间这种自愿的协作活动使得不同的网络运营商和 Internet 骨干网提供商能够分析并交换与攻击相关的数据。这种协作能够防止攻击行为升级并对重要系统造成破坏。

国土安全部将针对联邦政府与工业界及其他合作伙伴的合作而建设一个集中化的全天候联络点，这些合作包括网络空间分析、预警、信息共享、应急响应和国家级的恢复工作。私营部门对这些工作将起到主要作用，政府鼓励它们在法律允许的范围内加强合作，以便全天候地从宏观上掌握网络空间的安全程度。（A/R 1-1）

#### b. 扩大网络预警和信息网，以支持国土安全部对网络空间危机管理的协调工作

在危机管理中，几小时和几分钟的效果是截然不同的，如果花费几小时才处理完一个事件，则可能最终会导致大规模崩溃，而几分钟的快速处理则可使事件可控赢得了时间。要改善国家的预警能力，就要求为关键基础设施所有者和运营者以及他们的服务提供商之间的通信提供安全的基础设施。网络预警和信息网（CWIN）为政府和工业界提供了一个安全的带外专用通信

网络。这个网络还将包括电话会议及对数据的整合处理。

虽然 CWIN 的第一期工程只在联邦政府网络观察中心之间实现了通信，但 CWIN 的成员将最终包括关键政府部门和工业界的合作伙伴，如日常处理网络威胁的信息共享和分析中心 (ISAC)。随着这个领域内相关实体的扩大，其成员也会增加。对于 CWIN 成员，最重要的是有一个安全的、受保护的、可信的共享敏感网络攻击信息的环境。

根据 2003 年的预算，联邦政府将在政府内与网络安全相关的运行中心中安装 CWIN，以发布分析结论和预警信息，并实施危机管理的协调。联邦政府将考虑将 ISAC 连接到 CWIN 上。(A/R 1-2)

### (3) 国家级事件管理

增强国土安全部和私营 ISAC 的分析能力以及扩大 CWIN 将改善整个国家对网络事件的管理能力。然而，处理联邦政府内部网络事件仍需要国土安全部下属部门之外的其他组织的合作。例如，司法部、国防部和商务部在处理网络事件方面都承担着一一定的责任。在白宫也有很多办公室有责任参与对网络事件的响应，包括科技政策办公室（负责执行应急通信法令）、国家安全委员会（负责协调所有与国家安全和国际合作有关的事务）和 OMB。

另外，在适当情况下，州政府的首席信息官和国际实体也将参与对国家级事件的管理（见优先级 IV 和 V）。

### (4) 响应和恢复

#### a. 协调国家的公共-私营连续性和应急计划的开发

2001 年“9·11”事件之后，对安全分析得到的教训是联邦机构在通信和其他系统方面的应急能力很不协调，而且在很多情况下非常不完善。应急计划是网络安全的一个重要要素，若没有充分的应急计划和培训，则各个部门可能无法处理服务中断的情况，无法确保经济的持续发展。根据《联邦信息安全管理法》的规定，管理和预算办公室 (OMB) 是承担制定连续性计划的机构，并由总检查长协助进行该项工作。

#### b. 在联邦网络系统中实施网络安全连续性计划

在其他政府机构、州和地方政府的关键信息系统受到威胁或攻击时，国土安全部有责任就危机管理提供支持，如果私营机构提出类似请求，国土安全部也应给予支持。为了解整个国家对网络安全的准备情况，国土安全部将通过演练来检查民事机构在网络安全方面的有备性，这项活动与国防部的“合法接受者”演习类似。

为检查民事机构对网络安全的准备情况和连续性计划，国土安全部将通过演练来检查网络攻击可能会造成的影响。发现的弱点将被添加到矫正行动计划中，并提交给管理和预算办公室。国土安全部还将通过这种演练测试公共和私营机构在事故管理中的协调、响应和恢复能力。(A/R 1-3)

(i) 鼓励加强网络风险管理和业务连续性工作。非政府实体可以使用很多方法来管理网络带来的风险并制定业务连续性计划。风险管理包括风险评估、风险预防、风险减缓和风险保留。

没有什么特殊的技术可以确保企业的完全安全，不论各公司投入多少资本来改善其网络安全，都不可能防止有组织的攻击所导致的网络服务中断情况。对经济、健康、福利和公共安全有直接或间接影响的产品或服务的提供商已经开始使用网络风险保险项目以转嫁风险并提供业务持续性。

为较少网络攻击带来的损失并确保公司的运行和经济不受侵害，确保制定并测试充分的连

续性计划是一项重要的方法。

政府鼓励公司定期检查并演习信息技术连续性计划，把信息技术服务提供商的多样化（分散服务）作为一种降低风险的方法。（A/R 1-4）

（ii）推动公共-私营机构建设网络安全应急计划。要完全避免发生大范围的网络攻击是不太可能的，因此，对于确实已经发生的攻击，国家必须有一个综合的计划以对大规模的网络破坏和网络服务中断做出响应。有些机构在这方面有自己的计划，指明了在面临严重破坏的情况下如何恢复网络系统及其功能。但是，对于整个基础设施或从国家层面上，还没有一种机制来统一协调这些计划。

批准建立国土安全部的法令还为私营工业提供了可信的机制，规定可以使用 1950 年《国防产品法》的修订条款，即自愿性的战备规划条款，从而有利于私营部门制定自己的连续性计划。

鼓励基础设施部门为网络安全紧急事件建设互助项目。司法部和联邦商业委员会必须和这些部门一起消除这种合作中的障碍。另外，国土安全部的信息分析和基础设施保护署将协调制定并不断更新政府和工业界的自愿性网络安全连续性计划，包括恢复 Internet 功能的计划。（A/R 1-5）

## B. 信息共享

### （1）改善并增强公私机构在网络攻击、威胁和脆弱性方面的信息共享

提高分析、迹象发现和预警能力需要公私机构之间实施自愿的信息共享。网络空间安全事故及攻击信息的共享对于网络安全至关重要。现实存在的一些法律障碍使得有些组织不愿意与政府或其他组织共享这些信息。首先，有些组织担心与政府共享保密的、专属的或可能是令人难堪的信息可能会导致这些信息向公众公开。其次，在同一行业中公司间的竞争关系也可能会阻碍信息共享。最后，在有些情况下，可能只是因为缺乏高效的共享信息的机制。

批准建设国土安全部的法令为改善双向信息共享提供了几个特定的机制。首先，法律将确保企业自愿与国土安全部共享的关于威胁和脆弱性的数据不会以损害信息提供者的方式公开。其次，法律规定联邦政府在与私营企业共享信息或一起分析数据时必须依照保护涉密信息及其他敏感的国家安全信息的方法来保护这些数据。

按照法律，国土安全部在咨询相关的联邦部门后，将制定一个统一的接收、保管和存储流程，用来处理那些自愿提交给政府的关键基础设施信息。

这个流程将规定政府部门如何实施以下操作：

- 确认收到企业自愿提交的关键基础设施信息。
- 保存企业自愿提交的关键基础设施信息。
- 制定保管和存储这些信息的协议。
- 制定信息使用方法，使得既能够保护信息提供者的秘密，又能够使用这些信息来发布保护关键基础设施的预警。

公私机构之间对网络安全和基础设施脆弱性信息的共享存在着一些障碍，国土安全部将增强消除这些障碍的意识。国土安全部还将建设一个基础设施保护项目办公室，这个办公室将负责处理信息，还负责制定如何保管“企业自愿提交的关键基础设施信息”的协议。（A/R 1-6）

### （2）鼓励在更大范围对网络安全信息的共享

政府鼓励拥有大量计算机资源的非政府组织在信息共享方面发挥积极作用。公司、学院、

大学可以在发现和报告网络攻击事件、攻击方法和脆弱性方面发挥重要作用。特别需要指出的是，高新技术领域的公司和机构可以从增加网络安全信息共享上获益，参与者可以从 ISAC、FBI 的 Infragard 计划和美国联邦特工处电子犯罪特别小组等计划中获益。由于高新技术领域的机构拥有大量的计算机资源，这些资源可能会被利用来实施攻击，政府鼓励学院和大学为 Internet 服务提供商（ISP）和司法部门提供一个随时待命的联络点。

鼓励公司积极参与在业界共享 IT 安全信息的项目，包括参加适宜的 ISAC。建议学院和大学：（1）建设一个或多个 ISAC 以处理网络攻击和脆弱性；（2）为 Internet 服务提供商（ISP）和司法部门提供一个随时待命的联络点，在发现学校的 IT 系统即将实施网络攻击时通过该联络点与学校联络。（A/R 1-7）

## 6. 优先事务 II：国家网络空间安全威胁和脆弱性消减计划

网络上的恶意行为者可能是个人、犯罪集团、恐怖分子或国家。攻击者有很多种，他们都在寻求利用软件、硬件、网络和协议中存在的脆弱性以达到各种各样的政治或经济目的。随着我们对网络的依赖性越来越强，恶意人员可能造成的破坏面也越来越大。

等到知道恶意人员即将利用特定的脆弱性实施攻击才采取行动是一种危险的做法。并不是所有攻击发生前都能得到预警信息，而即使能够得到预警信息，有些脆弱性的矫正可能也会需要花几天、几星期，甚至几年的时间。因此，对于关键网络来说，必须在威胁出现之前找到并矫正脆弱性。最为危险的脆弱性必须优先处理，并以一种系统化的方法加以消除。

随着技术的更新和新系统的引进，我们的战略不可能消除所有脆弱性或震慑所有的威胁，我们将采取以下三项措施：

- （1）执行有效的计划以发现并制裁恶意行为者，从而达到减少威胁并震慑犯罪的目的。
- （2）寻找并矫正已知的最可能对关键系统造成破坏的脆弱性。
- （3）开发存在较少脆弱性的新系统，对新出现的技术实施评估以发现其脆弱性。

联邦政府无法单独完成这些任务，只能与州、地方政府和私营机构合作完成这些工作。很多联邦机构必须参与其中，这些机构的工作由国土安全部领导协调，是整个脆弱性消减计划的一部分。

本节将讨论这一项目的构成，包括联邦项目（现有的项目以及将提交预算审核的项目）以及联邦政府向其合作伙伴推荐实施的行动。政府将通过提高人们的意识以促使个人、公司和其他私营组织实施脆弱性消减计划，在“优先事务 III”中将描述用以提高安全意识的项目。

### A. 减少威胁和震慑恶意行为者

- （1）加强司法机构预防和起诉计算机犯罪的能力

《保护网络空间的国家战略》特别关注那些对网络基础设施实施破坏并可能对经济和安全造成严重破坏的威胁。通过发现那些可能造成严重破坏的威胁就可以减少对国土安全、国家安全和经济的威胁。司法机构和国家安全部门在防止网络攻击这一工作中发挥着关键的作用。司法机构还在对犯罪行为实施调查和审判并在断定攻击源方面发挥着核心角色。

很多基于网络的攻击是犯罪行为。根据司法部就计算机犯罪与知识产权方面的规定，负责追查罪犯并尽快对其实施审判的核心机构是 FBI 的网络处和联邦特工处。在攻击发生后，快速

反应可以遏制攻击的速度并最终减少其造成的损害。现在国家已有相应的法律和机制来确保能对大型事故迅速做出响应。理想情况下，在发生这种事件之后，必须对作案人员实施调查、逮捕和起诉。

然而，减少威胁并不只是对犯罪人员实施起诉这一种手段，分析并发布司法部门在调查中得到的实际信息将有助于提高国家基础设施的安全性。例如，通过 FBI 的 Infragard 计划、联邦特工处的电子犯罪特别工作组等几个计划，司法机构可以与私营部门共享从网络攻击中获得的经验教训。调查中收集到的信息可以为联邦政府和私营部门检查其网络安全提供一系列的技术，使得他们能够将有限的资源投入到处理其机构中特定的风险上。

司法部和 FBI 必须与国土安全部紧密合作，以确保它们能以适当的方式与 ISAC 及其他非政府实体共享在调查过程中收集到的信息，从而改善关键基础设施部门的风险管理能力。

国家将追查对网络实施攻击或试图实施攻击的人员并对其做出处理，从而达到防止、震慑和明显减少网络攻击的目的。对网络犯罪来说这项工作包括快速逮捕以及在适当情况下实施严厉的惩罚。

司法部和其他相关机构将通过以下方法来减少网络攻击和网络威胁：①设法改善从事关键基础设施和网络安全的联邦政府、州政府、地方政府的有关部门与私营企业之间在信息共享和调查协调方面的工作；②设法为调查和取证提供足够的资源和培训，以便快速调查并快速解决关键基础设施事故；③充分研究网络犯罪和入侵的对象，以掌握安全问题涉及的范围并及时跟踪情况的变化。(A/R 2-1)

(2) 制定国家脆弱性评估过程，以更好地了解威胁和脆弱性可能带来的后果

为更好地了解如何进一步发现并防止攻击，国家必须知道其面临的威胁是什么。到目前为止，并没有对战略性网络攻击可能导致的影响做过全面的评估。由于其他国家和恐怖分子正在加强网络攻击能力，因此很有必要研究这些攻击可能造成的影响以及消除其影响的可行方法。

国土安全部将协调适当的联邦机构和私营部门，对国家的网络威胁实施评估，确定各类目标可能造成的攻击影响。(A/R 2-2)

## B. 标识并矫正已有的脆弱性

减少脆弱性需要占用很多资源，因此，国家在标识并矫正脆弱性这项工作上必须采用成本有效及系统化的方法。美国必须消除网络的四个主要组成部分的脆弱性，包括：(1) Internet 的运行机制；(2) 数字控制系统/监督控制和数据采集系统；(3) 软件和硬件；(4) 物理基础设施和相关设施。这四个部分与国家的关键基础设施有着复杂的关系，消除这些重要领域的脆弱性将有助于减少关键基础设施和服务受到攻击的可能。

(1) 改善 Internet 机制的安全性

为加强 Internet 的安全，开发和实施保护机制是 Internet 的所有者、运营者和用户的共同责任。为确保 Internet 核心功能可以安全地发展，私营部门要起到领导作用。适当情况下，联邦政府将继续支持这些工作。其目标是开发出安全、强健的机制，使得 Internet 在现在和将来都能满足国家的需要。这包括加强 Internet 协议的安全性、加强负责转发数据的路由器的安全以及实施有效的管理机制。

a. 改善关键 Internet 协议的安全性和韧性

对于 Internet 基础设施安全性而言，最为重要的是确保以下三项关键协议的可靠性和安全



性：IP、DNS 和 BGP。

(i) IP。当前的 Internet 基于 IPv4 协议。有些组织和国家正转向新版的 IPv6 协议。IPv6 相对于 IPv4 有一些优点，除了提供大量的地址外，它在改善安全性方面也有新的特色，包括 IPSec 功能以及一些新的应用。有的国家在采用 IPv6 方面显得很积极，日本将在 2005 年实现将其网络基础设施改造为基于 IPv6 协议的目的

标，欧盟已经开始了采用 IPv6 的工作，中国也正考虑尽早采用 IPv6。

美国必须充分理解改用 IPv6 的优点以及这项工作的难点，并在此基础上制定改用 IPv6 的计划。联邦政府可以在其自己的网络上率先使用 IPv6，并协调相关私营部门参与这些行动，从而使得人们对这项工作更为理解。

商务部将组织一个特别工作组研究与 IPv6 相关的工作，研究内容包括政府在这项工作中的职能、国际合作、IPv4 到 IPv6 的安全转换、成本和利益。特别工作组将征求那些可能受影响的企业的意见。(A/R 2-3)

(ii) 加强 DNS 服务器的安全。DNS 将确保数据包通过 Internet 正确传输的中心数据库，如果无法访问该数据库或者该数据库受破坏后无法迅速恢复，则会导致信息无法正确传输。攻击者可以向 DNS 服务器发送大量的数据或请求，从而导致 DNS 服务器拒绝服务，或者通过入侵该系统对其数据实施破坏导致 DNS 服务器无法正常使用。2002 年 10 月 21 日，有攻击者攻击了支撑 DNS 服务的 13 个根服务器并使其性能下降或无法提供服务，这表明了 Internet 的一个脆弱性。出现这种攻击说明必须尽快采取措施使得这种攻击更难实施或无法造成严重后果。

(iii) 边界网关协议 (BGP)。在 Internet 上使用的各种路由协议中，BGP 是最可能受到黑客攻击并导致大规模拒绝服务的一种协议。BGP 用于连接数千个网络，从而构成整个 Internet，其作用是在不同的网络之间交换路由信息。这些网络可能是由不同的管理人员管理的，使用的管理策略或协议也可能不一样。

在 Internet 上传播错误的路由信息可以造成 Internet 的一部分甚至大规模的拒绝服务。例如，错误的路由信息可能造成“黑洞”，也就是使得发送到某个网段的数据包无法到达目标地址。这种攻击还可能在某些其他类的大型路由/交换系统中产生级联影响，即一个交换设备的错误将导致与其相连的网络出现错误，并进一步扩散，最终导致更大范围的错误。

采用更为安全的 BGP 和 DNS 服务对网络的所有者、运营者和用户都有好处。为解决这一问题，IETF（一个由 Internet 用户、所有者和运营者组成的自发性私营组织）组建了若干小组

### Internet 如何工作

在计算机之间传输的数据被分解为多个数据包，每个数据包都携带着地址信息和一部分消息，每个数据包单独传输并在接收方进行重组。有两个协议能够确保数据包顺利地通过复杂的网络传输，并保证数据包到达目的地时保持可以理解的格式。这两个协议是：(1) 传输控制协议 (TCP)，TCP 将数据分解为多个数据包并保证接收方能够正确地重组这些数据包；(2) 网际协议 (IP)。IP 将确保数据包经过正确的路由传输到目的地。这两个协议统称 TCP/IP。

IP 对所有的 Internet 应用都非常重要。数据包要根据 IP 地址传输，IP 地址是一串数字，域名系统 (DNS) 的作用是简化对 IP 地址的管理，它通过建设多个域以及一个层次化的管理框架将 IP 地址映射为容易理解的字符串、单词或数字。

来研究如何加强 BGP 和 DNS 的安全。这些小组已取得了一些进展，但是它们的工作受到了技术的制约，而且也缺乏必备的协调机制。

Internet 的安全性和运行的连续性在很大程度上取决于是否能够改用更加安全的 BGP 和 DNS。国家对如何促进这一工作非常关注，在私营部门的工作需要协调或者缺乏激励机制时，政府必须发挥推动这一工作的作用。

#### b. 改进 Internet 路由机制

Internet 路由器的一些设计特性使其相对来说更易于受到攻击，特别是通过拒绝服务消耗路由器的处理能力。通过采用地址检验和带外管理可以从根本上改善 Internet 的路由机制。

(i) 地址检验。当前对于如何减少拒绝服务攻击造成的影响几乎没有有效的解决方案，因为路由过程中没有对地址实施校验和审计，使得无法判断攻击的来源并实施过滤。目前 Internet 基础设施的一个最大的弱点就是没有对源地址实施检验。而对于抵抗很多攻击来说，使 Internet 基础设施能够过滤伪造源地址的数据包是至关重要的步骤。

(ii) 带外管理。之所以很难消除拒绝服务攻击的影响，是因为这种攻击导致了用于实施控制的数据无法到达路由器。独立的控制网络（通常称为带外管理链路）是一种能够用于抵抗拒绝服务攻击的技术手段。

国土安全部将考虑增加改善路由器安全的研究的必要性，包括采用新的技术或者改良数据传输方法以改善路由器安全。国土安全部将特别跟踪带外管理和地址过滤技术的进展，并将向政府部门和私营部门推荐一些操作流程，使其能够提高网络的效率和可用性。另外，国土安全部将和私营部门一起研究在现有技术条件下增强路由器安全性的最有效途径和难点。

#### c. 改进管理

对 Internet（包括该网络上的数据和支撑该网络的设备）采用较好的管理措施也可以在很大程度上提高 Internet 基础设施的安全。国土安全部将和 Internet 的所有者及服务提供商一起工作，研究并推广最好的管理经验。国土安全部还将特地与网络服务提供商一起制定一项公认的网络管理“行为规范”，这项工作将参考联邦通信委员会（FCC）中的网络可靠性和互操作性委员会（NRIC）等机构发布的文档。

国土安全部将和商务部及其他机构一起，协调公共机构和私营部门之间的合作，以促进相关机构：①采用更为安全的协议；②开发更为安全的路由技术；③采纳“行为规范”，包括网络安全管理和相关的合作方面的规范。国土安全部将支持这些工作，在必要的情况下提交相关的预算计划。（A/R 2-4）

#### (2) 推广使用可靠的数字控制系统/监督控制和数据采集系统

在过去的 20 年里，美国的很多行业迅速转向采用数字控制系统（DCS）以及监督控制和数据采集系统（SCADA）来管理和监控各种设备。DCS/SCADA 是基于计算机的系统，很多基础设施部门和行业采用它来远程管理原由手工处理的操作流程。几乎每个经济部门都采用了 DCS 和 SCADA，包括供水、运输、化学品、能源和制造业。DCS/SCADA 系统越来越多地使用 Internet 传输数据，而不是像以前那样使用封闭的网络。

确保 DCS/SCADA 的安全是一项重要的国家事务，破坏这些系统可能对公共健康和安全造成严重的影响。然而，以下几个因素使得加强这些系统的安全变得很复杂。首先，加强安全性需要在系统建设、研究和开发方面增加投资，而各个公司可能无法支付这些费用，或者就公司自身而言认为增加这些开销是没有必要的，这些研究需要由多个基础设施运营者或企业共同参与。其

次，现有技术的限制可能阻碍安全措施的实施。例如，DCS/SCADA 系统通常是需要少量供电的小型独立系统，在其体积和供电量的限制下，很多安全措施很难应用。另外，这些系统是以实时模式运行的，采用安全措施可能会降低其性能并对整个大的系统的同步造成影响。

在保护 SCADA 系统的安全上，私营部门和公共机构都必须发挥作用。国土安全部将协调能源部和其他相关部门一起与私营部门合作，确保各个行业的投资者和用户对 DCS/SCADA 系统的脆弱性以及利用这些脆弱性可能造成的后果有深刻的认识。对于 DCS/SCADA 系统的运营者，必须就 DCS/SCADA 相关软硬件的安全实施培训和上岗资格认证。另外，国土安全部将和私营部门一起制定相关的安全标准和安全政策。

开发足够的测试环境以及开发延迟极低的链路加密/认证、密钥管理和网络状态监控技术对于增强 DCS/SCADA 的安全都有很大的帮助。

国土安全部将协调能源部和相关机构，与各个行业合作，制定最佳实践措施，研究新的技术，以增强 DCS/SCADA 的安全性，判断最关键的 DCS/SCADA 站点并制定改善这些站点安全性的优先计划。(A/R 2-5)

### (3) 减少并矫正软件脆弱性

第三个关键安全事项是基础设施中软件脆弱性导致的安全问题，每天都有新的软件脆弱性被发现，攻击者可以利用这些脆弱性实施攻击。目前每年大约发现 3 500 个脆弱性，通常都是由相关的厂家发布补丁供人们下载以矫正这些脆弱性。

很多已知的脆弱性虽然有相关的解决方法，但是在很长时间内并未得到矫正。例如，多数网络攻击采用的是最常见的十种网络安全脆弱性，这是多个原因造成的。很多系统管理员没有受过足够的培训，可能也没有足够的时间去判断其系统需要安装什么补丁。很多需要打补丁的软件对一系列互联的系统都有影响，在给予打补丁之前必须经过很长时间的测试。如果系统是一个核心系统，可能很难关闭该系统去安装新的补丁程序。

关键基础设施上的未打补丁的软件使得这些基础设施容易遭到入侵。软件脆弱性还可用于传播蠕虫，这可能造成拒绝服务或其他严重的后果，这些脆弱性还可以被用于获取基础设施的控制权。改进对这些脆弱性的矫正速度、范围和效率对于公共部门和私营部门都非常重要。

有几种措施有利于改善当前的局面。首先，国家需要有一个更好的发现脆弱性的项目，这个问题较为复杂，因为发现脆弱性既有利于加快制定解决方案也可能助长攻击。其次，脆弱性信息的共享机构必须是独立于投资者、安全公司和公众的一个中立机构，政府现在正资助这类机构，但是资助的程度和方式还需要进一步研究。

国土安全部将和国家基础设施咨询委员会及私营部门一起制定发现脆弱性的计划和机制。(A/R 2-6)

加快发布软件补丁的另一个步骤是建设通用的测试床。在这些测试床上运行政府机构和公司常用的应用程序，可以帮助不同的用户对补丁程序可能造成的影响进行统一的一次性测试，这有助于加速补丁程序的应用。

总务管理局 (GSA) 将和国土安全部一起为联邦政府建设一个软件补丁信息交换站。国土安全部将和私营部门共享其经验，推动各个行业自愿参与为包括大企业在内的其他部门建设一个类似的信息交换站的工作。(A/R 2-7)

最后，必须寻找矫正脆弱性的最佳方法并与各个领域共享，包括系统管理员的培训需求、自动化工具的应用以及实施脆弱性矫正管理流程。国土安全部将和各个公共及私营实体一起制

定和传播这些方法。在网络产品出厂的默认配置中采用更为安全的配置则有助于用户更为安全地使用这些产品。

政府鼓励软件行业在其产品开发过程和默认安装时考虑更多的安全特性，包括：①在产品中加入提高用户安全意识的功能和特性；②易用的安全功能；③尽可能为安全相关的工作提供指南和最佳实践措施。(A/R 2-8)

#### (4) 理解基础设施的互依赖性并提高网络系统和通信系统的物理安全

当一个基础设施遭到破坏时，其他基础设施也常常会受到影响。甚至网络空间中的破坏性事件也会影响到物理空间，反之亦然。一列火车在巴尔的摩隧道出轨后，芝加哥的 Internet 的速度也受到了影响；而由于墨西哥州的某次篝火晚会破坏了天然气管道，硅谷内与 IT 有关的产品纷纷止步不前；地球上空数百英里处的卫星失控后，受到影响的银行客户便无法再使用其 ATM。

网络空间同时也有很多物理形式的表现，如通信和 Internet 网络就要靠建筑物和导线所支持。在设计和建造时，这些物理元素已经包含了冗余特性，可以避免单点故障。然而，运营商和服务提供商仍应彼此合作，共同分析其网络，增强网络的可靠性和冗余特性。联邦通信委员会（FCC）下的网络可靠性和互操作性委员会以及国家安全电信咨询委员会将参与这一工作，并标识政府在哪些方面的行为不利于增强国家的网络安全。

国土安全部将积极工作以减少关键基础设施之间的互依赖性和物理设施的脆弱性。

国土安全部将建设并领导公私合作联盟以发现不同部门之间的互依赖性，包括网络和物理上的互依赖性。这些合作联盟将制定脆弱性的消减计划，并与《国土安全国家战略》中提出的计划联合发挥作用。国土安全部的国家基础设施仿真和分析中心（NISAC）将支持这一工作，该中心将开发一套模型来描述网络和物理上的互依赖性所带来的影响。(A/R 2-9)

在接到请求或在必要时，国土安全部将支持信息系统网络的所有者或运营者以及网络数据中心制定系统矫正以及应急计划，以减少大规模物理破坏可能对上述网络的支撑设施造成的破坏，并制定限制访问关键设施的操作流程。(A/R 2-10)

### C. 开发带有较少脆弱性的系统，评估新兴技术的脆弱性

在国家采取措施以提高现有系统安全性的同时，还必须确保待建的网络系统和基础设施是安全的。随着我们的日常经济生活对网络基础设施的依赖性越来越大，这越发显得重要。未来的安全要求我们对网络空间安全这一课题做更多的研究并努力开发更为安全的产品。

#### (1) 对联邦的研发日程做优先级排序

与脆弱性的逐步增加相适应，联邦政府必须增加对下一代网络安全技术研究的投资。为确保未来几年研发的进展能与不断变化的技术环境相适应，必须确保投资计划的灵活性。

国家将优先考虑网络安全方面的研究并提供必要的资源。新一代的技术将使得 Internet 能够满足快速增长的通信需求和电子商务的需求，只有新一代的网络系统广泛建立起来之后，更为高级的网络应用才可能投入使用。因此，在国家的科研工作方面，必须优先支持将网络空间改造为一个安全的、高速的通信基础设施。这一工作中包含很多重大的研究，国家的所有部门和所有资金都必须优先考虑网络安全研究工作。

为满足这一要求，科技政策办公室（OSTP）的主管将协调这一开发工作，每年更新研发日程。在联邦政府的研发日程中，从 2004 财政年度及其后续几年里安排了前期（1~3 年）、中

期（3~5 年）和后期（5 年或更长）IT 安全研究计划。在所有工作中，当前优先考虑入侵检测、Internet 基础设施安全（包括 BGP 和 DNS 等协议）、应用安全、拒绝服务攻击、通信安全（包括 SCADA 系统加密和鉴别）、高保障系统和安全系统集成。（A/R 2-11）

为优化与私营部门相关的研究工作，国土安全部将提供足够的机制来协调高校、业界和政府的研发工作，在必要时将建设新的机制。（A/R 2-12）

网络安全研究工作的一个重要目标是开发高度安全、可信、具有较强自恢复能力的计算机系统。未来的计算机、Internet 或其他网络系统会变得非常可靠，就像现在使用电灯和自来水一样。

国家必须设法确保未来建设的网络基础设施自身就是安全可靠的，国家将在财政预算范围内，通过国家网络空间安全研究日程安排来开发高度安全可靠的系统。

政府鼓励私营部门在近期的研发工作中，优先考虑开发高度安全可靠的操作系统。如果这种系统开发完成并通过评估，联邦政府将考虑增加财政预算，增加对这类系统的定购量。（A/R 2-13）

另外，国土安全部将推动国家级的公共-私营合作项目，推广用以提高软件代码开发的完整性、安全性和可靠性的经验和方法，包括在开发过程中减少错误代码、恶意代码和后门的流程与步骤。（A/R 2-14）

## （2）评估并保护新兴系统的安全性

引入新兴技术就可能带来新的脆弱性，有些新兴技术带来的安全问题需要很长时间以后才得到修正，而且修正的难度很大，有时甚至根本无法修正。只要驾车到一个城市里兜一圈，就可以访问到很多无线局域网，而且不必知道这些无线局域网的所有者是谁，除非在这些系统中加入强安全措施。

随着电话、PDA 和很多其他的移动设施采用了更为高级的操作系统和上网功能，必须在这些设备中加入一些安全特性，以防止有人利用它们对无线网络甚至对 Internet 实施分布式攻击。

新兴研究领域还可能引入一些不可预知的安全问题，在这些技术中，光学计算的出现，更远的如纳米技术和量子计算的出现，都可能彻底改变当前的网络空间和网络安全问题。国家必须站在这些技术的最前沿并深入理解这些技术对网络安全带来的影响。

国土安全部将协调 OSTP 和其他相关的机构，促进公私研究机构以及安全界的交流，以确保新兴技术能定期接受国家科技委员会内相关部门的检查，查看其是否与国土安全和网络安全的要求相符，以及是否与联邦研究日程相符。（A/R 2-15）

## 7. 优先事务Ⅲ：国家网络空间安全意识和培训计划

政府鼓励网络空间中的用户都来帮助政府去保护各自能够影响或控制的网络空间。

为此，用户必须获知防止入侵、网络攻击以及其他破坏行为的基本知识。网络空间的所有用户都有责任保护网络的安全，不仅是为了其自身，而且是为了整个网络空间的安全和健康发展。

除了不了解现有信息系统的脆弱性之外，至少还有两个重要的因素阻碍了用户或管理人员采取行动来保护网络的安全：①缺乏对网络空间安全问题的了解，知识及认识程度不够；②缺乏足够受过培训或通过认证的系统安全人员。

本项优先事务包括以下内容：

- 实施一项全面的国家级意识培养项目，使得包括商人、普通员工、一般民众在内的所

有美国人都能够保护其自身所处的网络空间的安全。

- 实施足够的培训和教育项目，以支持国家网络空间安全的需求。
- 提高现有的联邦网络空间安全培训项目的效率。
- 推动私营部门对得到良好协调的、广为认可的网络安全专业认证体系的支持。

对任何成功的国家级网络空间安全工作来说，关键的是要提高人们（包括任何层次的用户和管理人员）的网络安全意识并拥有一支得到足够培训或经过认证的 IT 安全专家队伍。联邦政府自身无法承担或管理这一方面的所有工作，为做好这一工作，联邦政府必须与工业界、其他政府或非政府人员合作。

很多联邦机构必须参与这项工作，国土安全部在其中将承担领导和协调的角色。这一工作将包括以下联邦项目和活动（包括即将提交财政预算的项目和活动），联邦政府将向其合作伙伴推荐实施这些计划。

#### A. 意识培养

（1）实施一项全面的国家级意识培养项目，使得包括商人、普通员工、一般民众在内的所有美国人都能够保护其自身所处的网络空间的安全

在很多情况下，网络安全问题的解决方法是存在的，但是需要这些解决方法的人却并不知道这些方法或者不知道如何获得这些方法。有时人们甚至没有意识到必须保护网络的安全。例如，小型商业机构可能没意识到为其 Web 服务器设置默认口令可能会导致任何人都能控制该系统。在提高用户和操作人员对安全需求的敏感性上，教育和推广发挥着非常重要的作用。这些活动对于本战略中讨论的所有内容来说都是非常重要的组成部分，从工业界保护数字控制系统的安全，到家庭用户访问 Internet 的安全，教育和推广都将发挥着重要的作用。

国土安全部将与相关的联邦、州和地方实体以及私营部门相协调合作，推动全面的网络安全意识培养行动，其内容包括针对特定对象制定相应的培训教材，扩大“安全在线”（StaySafeOnLine）活动，面向工业界中为安全做出突出贡献的人员制定奖励项目。（A/R 3-1）

增强安全意识和增加培训将使得私营部门、各种组织和个人都能够保护其网络空间的安全。网络上一个实体的行动可以立即对其他实体产生很大的影响，因此，各个实体保护其自身网络空间安全的行动将对整个网络空间安全有很大的帮助。例如，近期一些被控制的计算机被用于攻击 Internet 上的 DNS 根服务器，使得大量的用户无法正常访问 Internet。通过提高网络安全意识，使得各个层次的用户增加对网络安全问题及其解决方法的了解，将促使他们行动起来保护网络空间的安全。国土安全部将领导一项用以提高用户的网络安全意识的工作。

##### a. 家庭用户和小型商业机构

家庭用户和小型商业机构不是关键基础设施的一部分，但是，他们的系统正越来越多被攻击者控制并用于攻击关键系统，因此，增强这些用户的安全意识将有助于进一步增强基础设施的安全。家庭用户和小型商业机构通常是对网络安全了解程度最低的人群。

国土安全部将与其他部门及私营部门合作，对普通的家庭用户、学生、小孩和小型商业机构实施培训，传授基础的网络安全知识。作为这项工作的一部分，国土安全部将和教育部及州和地方政府一起，在小学和中学中增加对网络安全的培训。另外，联邦贸易委员会将继续通过 <http://www.ftc.gov/infosecurity> 为消费者和小商业机构提供网络安全方面的信息。

国土安全部将和教育部一起，在合理的预算下，鼓励并支持州、地方和私营组织制定针对

中小学生学习网络安全的项目和指南。(A/R 3-2)

近几年，越来越多的用户使用“一直在线”的方式与 Internet 相连，如使用电缆 MODEM、DSL、无线上网或卫星系统，这使得家庭用户和小型商业机构的系统安全日益显得重要，其安全性不仅对这些用户自身非常关键，而且对于这些用户通过 Internet 所连接的系统也非常重要。例如，这些网络连接意味着可以发送更大数量的数据，而且可以以连续的数据流的方式，攻击者可以利用这些特点来对其他系统实施攻击，甚至可能对全国的网络造成严重的破坏。Internet 服务提供商、杀毒软件公司以及操作系统/应用软件开发商均可为家庭用户和小型商业机构提供商品和服务，这些机构有助于提高这些用户的网络安全意识。

家庭用户和小型商业机构可以通过保护自己的网络连接的安全以帮助提高国家网络空间的安全。个人或企业的计算机操作人员可以通过安装并定期更新防火墙软件、安装最新的杀毒软件、定期更新操作系统和应用程序以增强系统的安全性，这将有助于增强网络空间的安全性。为促进用户采取这些保护措施，国土安全部将组建一个由私营公司、组织和消费者群组成的工作组，通过该工作组，信息技术产品和服务的提供商或其他组织可以找到使家庭用户和小型商业机构更易于保护其系统安全的方法。(A/R 3-3)

#### b. 大型机构

大型机构的网络安全不仅对其自身非常重要，而且对于整个国家也很关键。大型机构拥有大部分的网络和计算机系统，随着经济活动之间的关联性日益增强，如果这些网络或计算机系统不安全，则可能被用于破坏其他经济活动。如果发生了大规模攻击的话，还可能会造成严重的经济后果。通过加强管理，使大型机构在各方面，特别是系统配置、身份鉴别、培训、应急响应和网络管理方面采用最佳的方法和高效的技术，这将能够改善大型机构的网络安全。国土安全部继续采取有关行动来提高这些网络的所有者对网络脆弱性的警觉性，并促使他们了解如何减缓这些脆弱性。国土安全部将与其他部门及私营组织一起，扩大现有的工作，以促使重要公司的决策者（CEO 和董事会成员）注意保护其公司的信息系统安全。

决策者可以采用一系列的步骤改善其机构的网络安全并保护其网络不被恶意利用。

鼓励大型机构对影响国家关键基础设施安全的内部网络的安全性进行评估。评估内容包括：①审计最佳实践措施的有效性及其应用；②制定连续性计划，考虑配备冗余人员和设备；③参与工业界范畴内的信息共享及对最佳实践措施的传播。(A/R 3-4)

**内部人员威胁。**很多对系统的网络攻击是由被认为是可靠的“内部人员”实施的。内部人员是指得到授权访问信息系统和网络的人员。但这些被认为可靠的人员可能会对该机构造成很大的威胁。内部威胁带来的风险很严重，因为那些试图破坏我们国家的人可能会因此而控制一些能便于他们达到恶意目的的系统。为了有效降低内部威胁可能带来的危险，离不开有关策略、实践措施和长期的培训。以下三项策略或能够减少内部人员威胁：①访问控制；②责任分离；③有效实施安全策略。

- 不健全的访问控制可能导致某些个人或团体以不适当的方式修改、破坏或泄露敏感数据，或者使用计算机程序来获取个人信息或制造破坏。
- 责任分离对于确保企业信息系统的完整性非常重要。不能允许任何人对任何系统有完整的控制权。
- 安全策略的有效实施是一项具有挑战性的工作，需要定期对实施情况进行检查。目前已经出现了一种新的自动化软件，能够有助于实施安全策略。这些程序可以以人类语

言的格式输入安全策略，并将这些策略转化为机器代码，然后依据这些策略对所有进出网络的数据在分组级别上进行监控，他们能够发现并制止滥用网络及其资源的情况。

#### c. 高等教育机构（IHE）

在增强高等教育机构的网络安全方面，提高安全意识将起到特别重要的作用。根据近期的经验，很多被联合攻击的不安全的计算机系统都可以追溯到高等教育机构的校园网络，它们是拒绝服务攻击或对 Internet 上其他系统造成威胁的平台。这些攻击不仅破坏了目标系统，也损害了这些系统所有者的利益以及希望使用这些系统来提供服务的用户的利益。高等教育机构之所以会成为攻击的目标，主要由于以下两个原因：（1）这些机构拥有大量的计算机资源；（2）这些机构允许外部在一定程度上访问其计算机资源。高等教育机构拥有的计算机资源非常庞大，超过了 3 000 多所学校，其中很多学校都拥有研究设施和大型的中央计算设施。

高等教育界已经发起了联合行动，积极地组织起了各成员，协调美国校园中的意识培养及网络安全增强工作。其中最引人注目的组织是 EDUCAUSE，这一组织与包括美国教育委员会和高等教育 IT 联盟在内的高等教育领导机构一起发起了与制定本战略有关的议题。这些工作取得了明显的效果，特别是各个大学的校长已经采纳了包含以下五个要点的行动框架，该框架要求他们优先考虑 IT 安全问题，并采取必要的政策和措施来实现更程度的系统安全：

- 在高等教育机构中优先考虑 IT 安全问题。
- 修订安全策略并改善对现有安全工具的使用。
- 改进未来的研究和教育网的安全性。
- 加强高校、企业和政府之间的合作。
- 将高校的工作和国家的工作结合起来，共同加强关键基础设施的安全。

鼓励各个学院和高校采取以下全部或部分安全措施来加强其网络系统的安全：①建设一个或多个 ISAC，以处理网络攻击和网络脆弱性问题；②制定相关策略，授权首席信息官处理网络安全问题；③为 IT 安全制定最佳实践措施；④制定模范的用户安全意识项目和教材。（A/R 3-5）

#### d. 私营部门

国土安全部将与私营部门一起解决普遍的网络安全意识问题以及可能对特定部门造成影响的某些议题。私营部门拥有并运营着国家网络空间中的绝大部分设施。作为保护网络空间的长期合作伙伴，很多私营部门已经制定了与本战略相应的保护计划，以保护其各自拥有的关键基础设施。在创建可影响多个基础设施部门成员的部门级意识培养项目方面，每个部门都要担当起重要角色，通过这些意识培养项目来消除脆弱性，各个成员可以共同研究并共享通用的安全解决方案。例如，SCADA 系统的安全是能源行业中广泛存在的网络安全问题，因此能源部要负责协调整个能源行业一起解决该问题。各部门还可以在标识研究需求方面发挥作用。国土安全部将与私营部门紧密合作来制定各部门自己的网络空间保护计划。

持续的公共-私营合作联盟将有助于通过以下工作来保护国家网络基础设施的安全：在必要和可行时参与对技术和研发的缺陷分析，从而能够对联邦的网络安全研究日程提供输入，对相关的研究进行协调，并制定和传播网络安全的最佳实践措施。（A/R 3-6）

#### e. 州政府和地方政府

国土安全部将实施有关计划来促使州和地方政府中的关键决策人员，如州长、州立法机构、市行政官和地方专员/管理委员会等支持对信息系统安全措施的投资，并促使他们采纳强制性的



管理政策和实践措施。

## B. 培训

除提高大众的安全意识之外，国家必须集中资源培训一批能够专门保护基础设施安全的、充满才干且具有创新能力的专业人才。随着 Internet、计算机和其他网络设备的广泛使用，对这类人才的需求正迅速增加，现有的培训投入已经无法满足需求。当前大学培养的工程人员较少，学校的大多数资源已经投入到其他学科，如生物和生命科学等上。如果美国希望通过其网络经济来领导全球发展，这一局面就必须得到改变。

(1) 培育足够的教育和培训项目，以满足国家网络安全的需求

改进网络安全培训的工作将主要由私营培训机构、教学机构以及国家的教育系统来承担。

国土安全部还将鼓励私营部门在工作场所提供足够的培训机会，对员工实施长期的教育和高级培训，以保持其较高的技术标准和创新能力。

联邦政府可以通过多种方式发挥直接作用。首先，国土安全部将实施并鼓励在美国国内制定用以推动网络安全专业培训的项目，包括与国家科学基金会 (NSF)、人事管理办公室 (OPM) 和国家安全局 (NSA) 相协调，一起探寻如何利用现有的“网络警察服务奖学金”项目以及由《网络安全研究和开发法》创建的为各类研究生、博士后、高级研究人员和教员提供的奖学金和受训项目。(A/R 3-7)

(2) 提高已有的联邦网络安全培训项目的效率

其次，国土安全部将考虑建设一个旨在开发网络安全培训措施的中心机构，该机构将收集起专家的意见，并与联邦的“一次建设、多次使用”的原则相符。

国土安全部将与具有网络安全培训知识的其他机构相协调，一起制定一种协调机制，将联邦政府的网络安全培训与计算机司法取证培训项目联系起来。(A/R 3-8)

## C. 认证

### 推动私营部门对得到良好协调的、广为认可的专业网络安全认证体系的支持

与教育培训相关的一个需求是合格人员的认证。认证可使得雇主和消费者能够对雇员及安全顾问的能力有更多的了解。目前已经有了一些网络安全认证项目，但是，这些认证对网络安全知识的要求很不一致。例如，有些认证强调广泛的网络安全知识并使用大量的多选题的方式实施测试，而有些认证则强调对某一方面的网络知识必须有深入的实践知识。还没有一种认证能够像医学和法律专业的认证那样，对人员的实践经验和理论水平提供一个合理的衡量标准。

为解决这一问题，包括 IT 安全认证供求双方的代表在内的很多相关人士已经开始考虑制定一个全国通用的网络安全认证体系和认证指南。

这些组织必须考虑的问题包括教育和经验水平的分层、不同认证机构对认证结果的互相承认以及认证标准、后续教育需求、面向各级认证的测试指南以及类似于其他领域中成熟的专业认证管理模式。作为认证的消费者（即雇用通过认证的人员），国土安全部和其他联邦机构可以有效而清晰地描述联邦 IT 安全机构的需求，以促进认证工作的开展。

国土安全部将鼓励为建设一个公私部门广泛认可的安全认证项目而开展必需的基础工作。国土安全部和其他联邦机构将有效而清晰地描述联邦 IT 安全界的需求，以协助这些工作的开展。(A/R 3-9)

## 8. 优先事务IV：保护政府部门的网络空间安全

虽然多数关键基础设施位于私营部门，但各级政府也承担着很多关键的职能，包括国防、国土安全、应急响应、税务、中央银行工作、司法和公众健康。所有的这些职能（以及其他职能）如今都依赖于信息网络和系统，因此，政府有责任保护自己的信息系统以确保它能够为人民提供最为基础的服务，对于联邦政府这一级的政府来说，这也是法律规定的一项职责。

要建立联邦政府网络安全的基石，就必须明确、清楚地为网络安全划定权责和责任，要求联邦政府的官员能履行这些责任并在财政预算和资本计划中考虑网络安全需求。

联邦政府将对网络安全问题给予必要的重视，以起到示范作用，并鼓励其他部门也采取这些措施。联邦政府还将通过其采购计划增强网络安全。例如，联邦政府在适当情况下必须率先采用新的更为安全的系统和网络协议。

州政府和地方政府对网络安全也可以有类似的影响，联邦政府将与州和地方政府合作来改善网络安全。

在联邦政府内，管理和预算办公室（OMB）主任负责确保各机构的领导执行了法律规定的 IT 系统安全职责。国家安全部门中的涉密系统则由国防部长和中央情报局局长负责。

### A. 联邦政府

自 2001 年 2 月的财政预算蓝图始，经过 2002 和 2003 财政年度预算计划以及“政府管理改革日程”，本届政府已经设立了一个清晰的改革日程表。这些改革包括统一联邦政府的安全和关键基础设施保护工作，并规定联邦政府对 IT 系统投资的前提是这些系统具有很强的安全性。

《保护网络空间的国家战略》将通过确保联邦政府能够发现脆弱性、预测威胁、尽可能减缓攻击以及提供运行持续性来支持这些改革。

为克服网络安全措施不足的问题，管理和预算办公室（OMB）依照法律制定了一项面向整个政府部门的 IT 安全项目，以确立 IT 安全政策并对联邦机构是否符合安全要求进行监督。这一项目将基于一种成本有效的、以风险分析为基础的方法，联邦各机构必须确保每项 IT 投资都考虑了安全问题。这一方法旨在促进联邦政府的业务运行，而不是对这些功能产生不必要的阻碍。

#### （1）不断评估联邦网络系统的威胁和脆弱性

确保联邦 IT 安全的第一步是了解各系统中的安全性和隐私控制机制的有效性。这之后，通过不断的风险评估周期来保持对情况的掌握也同样重要。管理和预算办公室（OMB）的安全政策对此已做出了规定，并在《联邦信息安全管理法》（FISMA）中做了特别规定。

OMB 就政府信息安全改革问题于 2002 年 2 月向国会提交了第一份报告，该报告指出了整个政府的安全绩效中存在的六项共同不足。

这些弱点包括：

- 高级管理层对此不重视；
- 缺乏对绩效的考核；
- 缺乏安全教育，安全意识不足；
- 在资金使用计划和投资控制方面没有充分考虑安全问题；

- 未能确保合同商服务的足够安全；
- 未能实现对脆弱性的检测、报告和信息共享。

这些不足并不是新问题，也不会令人感到惊讶，OMB 和审计总署（GAO）早在 6 年前便发现了这些情况。法律规定必须对联邦系统进行评估和报告，所以 OMB 和其他联邦机构便可利用这一机会为各机构的 IT 安全绩效制定一份此前尚没有的综合性的跨政府基线。更重要的是，通过制定并实施矫正计划，联邦政府可以通过统一的流程来跟踪这些不足的解决工作的进展。

在 OMB 批准某一信息系统的建设资金之前，该系统的所属部门必须证明其已解决了该系统中最为明显的安全问题。另外，各机构还必须确保系统中已经融入了安全性，并且 IT 投资中每项安全成本均已通过联邦的资金规划流程得到了汇报。OMB 的政策中规定，必须标识系统中具体的生命周期安全成本，并作为系统投资的一部分得到资金赞助；否则，整个系统的资金申请将不会得到批准。

## （2）联邦机构中的几项专门步骤

联邦政府必须有一套全面、横向的增强网络安全的方法。改进和维持联邦政府中各机构的网络安全的三项核心步骤是：标识并记录联邦机构的体系结构；不断评估威胁和脆弱性，并了解威胁和脆弱性对机构的运行和财产可能带来的风险；实施安全控制和脆弱性矫正措施，以降低或管理这些风险。每个联邦机构必须制定并实施这三个步骤，从而实现更加稳固的安全。

### a. 标识并记录联邦机构的体系结构

OMB 的政策要求每个联邦机构标识并记录其体系结构，包括对其所有资产和业务、所有 IT 系统、关键业务流程、与其他机构的关系等都要有一个官方的正式清单。该步执行后便可以了解整个政府机构的关键性安全需求。

通过财政预算流程，联邦政府将促使各个联邦机构购买商用网络安全工具来改善其体系结构和系统配置。配置管理和控制对于提高安全性有着显而易见且重要的作用。例如，对系统配置实施控制后，可以使各个部门能够更为有效和高效地实施安全策略和权限控制，更容易在整个系统或网络上安装防毒软件及其他软件的升级版本或补丁程序。

### b. 不断评估威胁和脆弱性

应使用商用的自动化审计和报告机制来验证系统中安全控制的有效性，这对持续地把握系统风险至关重要。这些工具可以帮助来分析数据、提供前瞻性评估并对机构运行中不可接受的风险提出警告。

联邦机构将继续扩大对自动化的安全评估和安全策略实施工具的使用，并积极部署威胁管理工具，从而能够检测到攻击。联邦政府将判断是否必须采取特定的措施（通过政策或财政预算流程）来促使各个机构更多地使用这些工具。（A/R 4-1）

### c. 实施安全控制和脆弱性矫正工作

安全控制可将风险维系在可接受的级别，这些控制往往可以在一段相对较短的时间内实现，然而矫正脆弱性则是一个更为复杂的问题。软件总在不断发生变化，每次升级都可能带来新的脆弱性，因此必须不断地对脆弱性实施评估。矫正过程通常包括“打补丁”或者安装一些软件或代码来更新主程序。联邦系统的矫正工作必须时常做出规划。

## B. 整个政府面临的其他挑战

联邦政府还面临着其他四项特定的安全问题需要处理，每个有关部门都必须与 OMB 一起

合作来对其解决。

### (1) 联邦系统用户的鉴别及对授权的维护

标识并鉴别每个系统用户是网络安全链上的第一环，每当用户被授权访问系统时都必须实施身份鉴别。为实现并保持系统的运行安全，每个机构必须确保系统上的用户的确是它们所声称的身份，且它们只在做授权可做的事情。当前使用的很多鉴别流程不够安全，如系统的默认配置口令没有得到修改、口令没有正确配置、口令很少更新等情况。

联邦政府将继续为所有的联邦雇员及流程提供一个连续的安全链，包括在适当的情况下使用基于生物特征的智能卡来访问建筑物或计算机，并在用户登录计算机之始就对其身份实施鉴别。上述方法的益处是显而易见的。通过使用多重的身份标识和鉴别措施——强口令、智能卡以及生物特征等，联邦政府将消除当前很多严重的安全问题。

通过现在正在实施的电子鉴别活动，联邦政府将审查对强访问控制和身份鉴别的需求，研究联邦各部使用相同的物理和逻辑访问控制工具及鉴别机制的范围，最终进一步推动一致性和互操作性。(A/R 4-2)

### (2) 保护联邦的无线局域网

在使用无线技术时，联邦政府将仔细评估在关键功能上使用这些技术可能带来的风险。国家标准与技术研究院 (NIST) 已发表声明说无线通信可能会遭到拦截，且无线网络也可能受到拒绝服务攻击。联邦机构应当将 NIST 对无线系统的看法和建议作为无线网络运行的指南。

联邦机构应当考虑安装能持续检测非授权网络连接的系统，各个机构的政策和流程应当反映出对风险消减措施的考虑，包括使用强加密技术、双向鉴别、防辐射标准及技术、配置管理、入侵检测、事件处理、计算机安全意识与培训项目。(A/R 4-3)

### (3) 改进政府外包和采购的安全性

通过 OMB 的联邦采购政策办公室、联邦采购规则委员会以及行政管理部门信息系统安全委员会的共同努力，联邦政府正在寻找能改进政府部门合同安全的方法，并评估了整个联邦采购流程与安全的相关性。在 2002 年 2 月 OMB 向国会

#### 国家信息保障联盟 (NIAP)

美国政府建设 NIAP 的目的是满足 IT 产品的厂商和消费者对安全产品实施测试、评价和评估的需求。NIAP 是国家标准与技术研究院 (NIST) 与国家安全局 (NSA) 在实施 1987 年《计算机安全法》规定的各自职责的过程中联合建设的。

这一联盟于 1997 年建立，它综合了上述两个机构在网络安全方面的经验，就 IT 产品和系统在网络安全方面的技术需求以及对这些产品的评估方法开展了研究。NIAP 的长期目标是通过成本有效性合理的测试、评价和评估项目增强消费者对信息系统和网络的信任。NIAP 将在多个领域继续与政府部门和工业界建立密切的合作关系，旨在帮助解决当前或未来可能对国家信息基础设施造成影响的安全问题。关于该联盟的更多信息可以参考 <http://www.niap.nist.gov>。

提交的安全报告中，指出了政府机构中的外包安全性是一个重要的安全问题。

联邦政府将对国家信息保障联盟 (NIAP) 重新进行全面的考查，以判断其对商用软件产品中不断出现的安全缺陷这一问题的解决程度。这一考查过程将吸取在实施国防部 2002 年 7 月发布的政策时得到的教训——该政策要求产品在采购时应经过 NIAP 或类似评估流程的审

查。(A/R 4-4)

国防部的政策规定,如果所需的产品类中已有通过评估的产品,则国防部下属部门必须购买通过评估的产品;如果所需产品类中还没有通过评估的产品,则该部门必须要求备选的产品提供商将其产品提交给评估机构,以便国防部进一步考虑是否购买其产品。

在完成对 NIAP 的重新考查之后,政府将研究把该项目推广到所有联邦机构时的成本有效性。如果可行,它将既能增强政府的安全性,又能够最大可能地利用政府强大的购买力对市场产生影响,并因此能改善所有 IT 产品的安全性。

#### (4) 为独立的安全审查和认证制定专用标准

随着对安全的重视程度的增加,相应地需要对联邦各机构的安全项目和活动进行专业化的独立验证和确认。FISMA 和 OMB 制定的实施指南中已规定各机构的项目负责官员及 CIO 至少每年审查一次该机构的安全项目。但很少有机构具备实施这些审查工作的人力资源,因此它们一般是将此项服务外包出去。各机构及 OMB 均发现承包商的安全水准参差不齐,有些是真正的安全专家,而有些则不尽如人意。另外,很多负责独立验证和确认安全项目的承包商同时还是安全项目的实施方。因此,它们在审查项目时可能会偏向于选择对它们有利的安全项目实施方法。

联邦政府将考虑是否有必要对联邦政府的安全服务提供商进行认证,以考查其是否具有最小的能力,包括考查其是否具有足够的独立性。(A/R 4-5)

### C. 州政府和地方政府

美国的民主政治根植于联邦制的概念,这种政府体系将政府的权力在联邦和州之间进行了分配。相互重叠的联邦、州和地方政府的管理权限导致了美国各级政府总共拥有超过 87 000 种不同的司法权,为网络安全工作带来了独特的机遇和挑战。与联邦政府一样,州政府和地方政府也运行着庞大的互联信息系统,这些系统支撑着其关键的政府职能。

美国各州提供的服务构成了数百万美国人民和家庭的“公共保安网”。这些服务包括重要的社会保障活动以及关键性社会保安职能,如执法和应急响应服务。各州还拥有并运营着很多关键基础设施系统,如电能和传输系统、运输系统、供水系统等。它们扮演了一种催化作用,能够把州内提供各项关键服务的各方召集到一起,共同对发生的危机进行防备、响应、管理,并从危机中实施恢复。在我们的联邦系统中,州政府提供的关键服务使其担负着特殊的角色和责任,使州政府因此而成为一个关键基础设施部门。

由州政府实施的很多这样的关键职能都必然地与 IT 紧密相连,包括福利金的提供、因执法目的而以电子手段访问犯罪记录、州政府的公共事业和运输服务的运转。我们要能够阻止攻击,或在攻击事件发生时迅速响应,这样才可确保这些服务能全天可用,才可提供公众所需要和期望的关键服务。IT 系统可以为各州内的居民提供空前高效的服务和响应,公民对这些 IT 系统以及这些系统上收集并存储的数据的完整性所持的信心是很重要的,它能使这些 IT 系统的优越性得到进一步的体现和充分利用。

随着对集成系统的不断依赖,州、地方、联邦机构不得不联合起来对付网络攻击。对系统的保护信息的共享对于确保政府的连续性来说是很重要的基础。各州已经采取了很多机制来促进对网络攻击信息的共享以及对攻击事件的报告。

当新的政策出台以及新的技术解决方案出现时,这些机制还要不断地更新和改善。除此之

外，州政府正在探索某些方法来改善对内、对外的信息共享。这些方法包括以立法的形式为网络安全提供进一步的资金和培训项目，还包括在州、地方、联邦政府之间组建合作联盟来共同对付网络威胁。

国土安全部将与州和地方政府合作，鼓励它们考虑制定 IT 安全项目并与情况类似的州一起参加 ISAC。

鼓励州和地方政府为其各个部门和机构制定 IT 安全项目，包括意识培养、审计及标准；鼓励各州与其他情况类似的州一起参加已经建立的 ISAC。(A/R 4-6)

## 9. 优先事务 V：国家安全和国际网络空间安全合作

美国的网络空间是国际网络空间的一部分，网络攻击正以光速跨越国界，很难实时识别来自罪犯、国家和恐怖分子的攻击行为，这便要求美国应当准备好保卫其关键网络并对每次事件中的攻击都做出响应。用于支撑国家重点国防设施和情报机构的系统必须是安全、可靠和有韧性的，即能经受源自任何地方的攻击。美国还必须做好准备，在必要时能针对其关键基础设施遭遇的攻击做出响应。同时，美国还必须随时准备领导全球工作，与各政府和相关行业一起保护那些对世界经济和市场的运转而言至关重要的网络空间。全球性的安全工作要求提高安全意识，推广更加强健的安全标准以及积极调查和起诉网络犯罪。

### A. 确保美国的国家安全

我们面对的敌人包括敌对国家和恐怖分子，他们均可能实施网络攻击或试图利用我们的系统。在和平时期，美国的敌人可能对我们的政府、大学的研究中心和私营公司开展间谍活动，他们也可能预先摸清美国信息系统的情况、选择重要的目标并安装后门或其他访问渠道以袭击我们的基础设施。在战争或危机时期，敌人可能攻击关键基础设施和重要的经济功能，或打击公众对信息系统的信心，以达到威胁恐吓的目的。他们还可能通过干扰国防部、中央情报局及其他政府机构和关键基础设施来降低美国军队的反应能力。

美国已经经历过几次重大的国家网络安全事件。1998 年，攻击者对国防部、国家宇航管理局（NASA）和政府的研究实验室发起了一系列熟练的、组织周密的网络入侵，目标是那些进行大气和海洋研究以及航空航天设备设计等与国家安全密切相关的高级技术研究机构。

美国必须拥有保护与国家安全紧密相关的系统和基础设施的能力，并且要发展快速标识恶意行为来源的能力。必须改善我们在网络空间中的国家安全状况，从而限制对手进行间谍活动或者对美国施压的能力。

#### (1) 加强网络空间中的反情报工作

联邦调查局和中央情报局应当确保以更强有力的反情报姿态来打击针对美国政府、商业和教育机构的以网络空间为基础的情报收集行为。这项工作必须包括要更加深入地了解我们的对手利用网络空间进行间谍活动的能力和意图。(A/R 5-1)

#### (2) 改善攻击源调查和响应能力

情报部门、国防部和执法机构必须增强迅速调查攻击源的能力，以便于及时有效地做出响应。与国家安全战略一致，这些工作同样将努力发展相关能力来抵抗对关键系统和基础设施的攻击。(A/R 5-2)

### (3) 改善美国国家安全部门对网络攻击响应的协调能力

美国必须增强与网络攻击和间谍活动有关的执法部门、国家安全部门和国防部门之间的协调能力，确保各个部门之间在适当情况下能够互相交换与犯罪事件相关的信息。国家安全委员会和国土安全办公室将对此进行研究，以确保相应的协调机制到位。(A/R 5-3)

### (4) 保留以适当方式回应的权力

当某个国家、恐怖主义集团或者其他敌人通过网络空间攻击美国时，美国政府的回应不需要局限于对犯罪活动进行起诉。美国保留以适当的方式进行回应的权力，美国将为这类意外事件做好准备。(A/R 5-4)

## B. 国际协作

美国国务院将承担加强国际网络空间安全协作的任务，主要的活动包括以下内容。

### (1) 通过国际组织与业界合作倡导和推广全球的“安全文化”

美国对推动网络空间安全的兴趣已经超越了其国界。其关键的国内信息基础设施均有向加拿大、墨西哥、欧洲、亚洲和南美的直接连接，国家的经济与安全依赖于遍布全球的美国企业、军事力量以及国外的贸易伙伴，而反过来，上述的机构同样也需要依赖于安全可靠的信息网络来工作。大量的网络空间攻击来源于国外的系统，或经由国外系统，甚至跨越了多个国界，我们需要国际合作来打击这些攻击。

支撑关键经济和安全运行的全球网络必须是安全和可靠的。保护全球网络空间的安全需要国际社会在提高安全意识、增强信息共享、推广安全标准以及调查和起诉网络犯罪方面进行广泛合作。美国承诺要与其他国家合作，以确保支撑关键经济和安全基础设施的全球信息网络的完整性。我们还准备利用政府资助的组织，如经济合作与发展组织（OECD）、八国集团（G-8）、亚太经合论坛（APEC）、美国国家州组织（OAS）以及其他相关组织等，以推动全球网络安全的协作。为了促进与私营机构的合作，我们还准备利用泛大西洋商业对话（TBD）这类组织。

### (2) 建设安全网络

为确保信息系统的安全性，并促进重要知识的共享，美国将参与一系列合作工作，解决在保障信息网络的完整性过程中遇到的各种技术的、科学的以及政策的问题。主要活动将包括鼓励制定和采纳国际技术标准，并促进世界上最优秀的科学家和研究者之间的合作和研究。美国还将通过很多努力来在新的信息社会的所有参与者之间灌输“安全文化”，如 OECD 的《信息系统和网络安全指南》。

大多数国家的关键信息基础设施掌握在私营部门手中，所以美国将鼓励其工业界参与上述工作，同其国外同行展开对等的对话，从而达到一举两得的目的：取得网络空间安全方面的有效案例；展现网络空间安全中与政府合作的成功途径。

美国政府将通过适当的国际组织加强合作，与企业建立合作联盟，以推动国外公共-私营部门间就信息基础设施保护展开对话，并推动全球“安全文化”的形成。(A/R 5-5)

### (3) 推动北美的网络空间安全

美国将与加拿大和墨西哥合作，将北美打造成“安全的网络空间地带”。我们将会把该项目扩展到标识和保护那些用来支撑电信、能源、运输、银行与金融系统、应急服务、食品、公众健康和供水系统的关键公共网络。(A/R 5-6)

### (4) 促进建设全国性和国际性的观察和预警网络，在网络攻击甫一出现便将其检测并预防

美国将督促每个国家在处理千年虫问题的经验基础上为国内和国际之间的网络安全工作指定集中化的联系地址。这些联系地址的建立能够极大地增强国际协作能力以及对问题的解决。我们还将督促每个国家都建立自己的观察和预警网络，用于向政府部门、公众和其他国家对可能发生的攻击或病毒发出通知。(A/R 5-7)

为了促进在出现网络威胁时的实时信息共享，美国将支持建立能够接收、评估和发布此类信息的全球网络。该网络可由 FIRST 之类的非政府机构负责建设。(A/R 5-8)

美国政府鼓励区域性组织，如 APEC、EU 和 OAS 等，分别建立或指派负责网络安全事务的委员会。这类委员会也可以通过与来自私营部门的代表共同建立联合工作组受益。美国政府还鼓励区域性组织，如 APEC、EU 和 OAS 等，与来自政府和私营部门的代表建立网络安全事务联合委员会。(A/R 5-9)

(5) 鼓励其他国家接受《欧洲委员会计算机犯罪约定》，或确保其法律和流程至少包含相关内容。

美国将大力支持调查和起诉网络犯罪的国际合作。美国已经签署并支持最近达成的《欧洲委员会计算机犯罪约定》。这一约定要求各国将网络空间攻击视为确凿无疑的犯罪行为，并通过采取流程措施以及相互间协助来更好地打击国际间的网络空间犯罪。

美国将鼓励其他国家接受《欧洲委员会网络犯罪约定》，或确保其法律和流程至少包含了相关内容。(A/R 5-10)

现行的多边工作，如 G-8、APEC 和 OECD 的工作也同样重要。美国将落实这些论坛上达成的建议和行动计划。在这些动议中，美国将特别督促其他国家加入 G-8 发起的 24 小时高技术犯罪联系网，目前该网络已经扩展到欧洲委员会的成员国以及其他国家。

## 10. 总结：前方之路

今后，我们对网络空间的依赖性仍将继续增加，网络空间和与之相联的网络正支撑着美国的经济，并为我们提供了国防和国土防御能力。这种国家依赖性必须通过持续的工作加以管理，以保护美国基础设施的网络控制系统。

保护网络空间是一项复杂而又不断变化的艰巨任务。《保护网络空间的国家战略》是在与依赖于网络空间的各个关键经济部门、州和地方政府、学院和大学及相关组织的紧密合作的基础上制定的。联邦政府曾经在全国举办了多次市政会并发布了 53 个关键问题供公众讨论。另外还公布了《保护网络空间的国家战略》的草案以听取公众的建议并引起了广泛的关注。

根据总统的号召建立起来的公私合作联盟已经制定了相应的战略来保护其成员所依赖的网络空间。这一独特的联盟关系还将继续发挥作用，因为国家大部分网络资源由政府之外的实体控制着。为使得这部战略能够发挥作用，必须确保国家的各个行业都有所投入并执行该战略，因此，还必须继续就如何保护网络空间在各个行业间开展对话。

《保护网络空间的国家战略》指出了五项有助于实现这一远大目标的优先事务，分别是：①国家网络空间安全响应系统；②国家网络空间安全威胁和脆弱性消减项目；③国家网络空间安全意识和培训项目；④保护政府部门的网络空间安全；⑤国家安全和国际网络空间安全合作。这五项优先事务将起到防止和震慑攻击并保护系统免受攻击的作用。另外，还可在发生攻击时使其危害降到最低点并使系统迅速恢复正常运行。



然而,《保护网络空间的国家战略》只是保护信息基础设施这一长期工作的第一步。联邦政府的行政机构将使用一系列的工具来实施这一战略。政府和国会将依照这一战略制定联邦政府未来在网络安全方面的财政预算,为每个与网络安全有关的机构提供执行其职责时所需的资源。每个领导部门和机构将制定自己的规划和项目来实施《保护网络空间的国家战略》为之部署的工作。

在联邦政府内部,国土安全部将在实施《保护网络空间的国家战略》中发挥核心作用。在完成本部门被分配的工作之外,国土安全部还将在与网络空间安全相关的事务上担当起州和地方政府、私营部门及公众的中心联络点。通过与白宫合作,国土安全部还可以协调并实施《保护网络空间的国家战略》中不属于联邦政府的任务。

每个部门和机构还必须为其在网络安全工作中的绩效负责,联邦政府将对各机构的绩效进行考核以评估本战略中描述的网络空间安全项目的有效性,同样鼓励州和地方政府亦如此。对绩效的考核还有助于各机构合理地控制进度、分配资源并调整工作的优先级。

联邦、州和地方政府以及美国所有的组织和人民将继续努力增强网络空间安全。随着这些战略和计划的实施,我们将逐步消减威胁和脆弱性。

网络安全和个人隐私并不矛盾,网络空间安全项目必须加强而不是减少对个人隐私的保护。联邦政府将继续与隐私保护倡议者定期会晤,同他们讨论网络空间安全问题以及本战略的实施情况。

在可以预见的未来,以下两件事是毋庸置疑的:一是美国将继续依赖网络空间,二是联邦政府将寻求建立一个持续、广泛的合作联盟来制定、实施并改善本部战略。

## 附录 行动与建议(A/R)概要

### 优先事务 I: 国家网络空间安全响应系统

**A/R 1-1:** 国土安全部将针对联邦政府与工业界及其他合作伙伴的合作而建设一个集中化的全天候联络点,这些合作包括网络空间分析、预警、信息共享、应急响应和国家级的恢复工作。私营部门对这些工作将起到主要作用,政府鼓励它们在法律允许的范围内加强合作,以便全天候地从宏观上掌握网络空间的安全程度。

**A/R 1-2:** 根据 2003 年的预算,联邦政府将在政府内与网络安全相关的运行中心中安装 CWIN,以发布分析结论和预警信息,并实施危机管理的协调。联邦政府将考虑将 ISAC 连接到 CWIN 上。

**A/R 1-3:** 为检查民事机构对网络安全的准备情况和连续性计划,国土安全部将通过演练来检查网络攻击可能会造成的影响。发现的弱点将被添加到矫正行动计划中,并提交给管理和预算办公室。国土安全部还将通过这种演练测试公共和私营机构在事故管理中的协调、响应和恢复能力。

**A/R 1-4:** 政府鼓励公司定期检查并演习信息技术连续性计划,把信息技术服务提供商的多样化(分散服务)作为一种降低风险的方法。

**A/R 1-5:** 鼓励基础设施部门为网络安全紧急事件建设互助项目。司法部和联邦商业委员会必须和这些部门一起消除这种合作中的障碍。另外,国土安全部的信息分析和基础设施保护

署将协调制定并不断更新政府和工业界的自愿性网络安全连续性计划，包括恢复 Internet 功能的计划。

**A/R 1-6:** 公私机构之间对网络安全和基础设施脆弱性信息的共享存在着一些障碍，国土安全部将增强消除这些障碍的意识。国土安全部还将建设一个基础设施保护项目办公室，这个办公室将负责处理信息，还负责制定如何保管“企业自愿提交的关键基础设施信息”的协议。

**A/R 1-7:** 鼓励公司积极参与在业界共享 IT 安全信息的项目，包括参加适宜的 ISAC。建议学院和大学：（1）建设一个或多个 ISAC 以处理网络攻击和脆弱性；（2）为 Internet 服务提供商（ISP）和司法部门提供一个随时待命的联络点，在发现学校的 IT 系统即将实施网络攻击时通过该联络点与学校联络。

#### **优先事务 II：国家网络空间安全威胁和脆弱性消减计划**

**A/R 2-1:** 司法部和其他相关机构将通过以下方法来减少网络攻击和网络威胁：（1）设法改善从事关键基础设施和网络安全工作的联邦政府、州政府、地方政府的有关部门与私营企业之间在信息共享和调查协调方面的工作；（2）设法为调查和取证提供足够的资源和培训，以便快速调查并快速解决关键基础设施事故；（3）充分研究网络犯罪和入侵的对象，以掌握安全问题涉及的范围并及时跟踪情况的变化。

**A/R 2-2:** 国土安全部将协调适当的联邦机构和私营部门，对国家的网络威胁实施评估，确定各类目标可能造成的攻击影响。

**A/R 2-3:** 商务部将组织一个特别工作组研究与 IPv6 相关的工作，研究内容包括政府在这项工作中的职能、国际合作、IPv4 到 IPv6 的安全转换、成本和利益。特别工作组将征求那些可能受影响的企业意见。

**A/R 2-4:** 国土安全部将和商务部及其他机构一起，协调公共机构和私营部门之间的合作，以促进相关机构：（1）采用更为安全的协议；（2）开发更为安全的路由技术；（3）采纳“行为规范”，包括网络安全管理和相关的合作方面的规范。国土安全部将支持这些工作，在必要的情况下提交相关的预算计划。

**A/R 2-5:** 国土安全部将协调能源部和相关机构，与各个行业合作，制定最佳实践措施，研究新的技术，以增强 DCS/SCADA 的安全性，判断最关键的 DCS/SCADA 站点并制定改善这些站点安全性的优先计划。

**A/R 2-6:** 国土安全部将和国家基础设施咨询委员会及私营部门一起制定发现脆弱性的计划和机制。

**A/R 2-7:** 总务管理局（GSA）将和国土安全部一起为联邦政府建设一个软件补丁信息交换站。国土安全部将和私营部门共享其经验，推动各个行业自愿参与为包括大企业在内的其他部门建设一个类似的信息交换站的工作。

**A/R 2-8:** 政府鼓励软件行业在其产品开发过程和默认安装时考虑更多的安全特性，包括：（1）在产品中加入提高用户安全意识的功能和特性；（2）易用的安全功能；（3）尽可能为安全相关的工作提供指南和最佳实践措施。

**A/R 2-9:** 国土安全部将建设并领导公私合作联盟以发现不同部门之间的互依赖性，包括网络和物理上的互依赖性。这些合作联盟将制定脆弱性的消减计划，并与《国土安全国家战略》中提出的计划联合发挥作用。国土安全部的国家基础设施仿真和分析中心（NISAC）将支持这

一工作，该中心将开发一套模型来描述网络和物理上的互依赖性所带来的影响。

**A/R 2-10:** 在接到请求或在必要时，国土安全部将支持信息系统网络的所有者或运营者以及网络数据中心制定系统矫正以及应急计划，以减少大规模物理破坏可能对上述网络的支撑设施造成的破坏，并制定限制访问关键设施的操作流程。

**A/R 2-11:** 为满足这一要求，科技政策办公室（OSTP）的主管将协调这一开发工作，每年更新研发日程。在联邦政府的研发日程中，从 2004 财政年度及其后续几年里安排了前期（1~3 年）、中期（3~5 年）和后期（5 年或更长）IT 安全研究计划。在所有工作中，当前优先考虑入侵检测、Internet 基础设施安全（包括 BGP 和 DNS 等协议）、应用安全、拒绝服务攻击、通信安全（包括 SCADA 系统加密和鉴别）、高保障系统和安全系统集成。

**A/R 2-12:** 为优化与私营部门相关的研究工作，国土安全部将提供足够的机制来协调高校、业界和政府的研发工作，在必要情况下将建设新的机制。

**A/R 2-13:** 政府鼓励私营部门在近期的研发工作中，优先考虑开发高度安全可靠的操作系统。如果这种系统开发完成并通过评估，联邦政府将考虑增加财政预算，增加对这类系统的定购量。

**A/R 2-14:** 国土安全部将推动国家级的公共-私营合作项目，推广用以提高软件代码开发的完整性、安全性和可靠性的经验和方法，包括在开发过程中减少错误代码、恶意代码和后门的流程与步骤。

**A/R 2-15:** 国土安全部将协调 OSTP 和其他相关的机构，促进公私研究机构以及安全界的交流，以确保新兴技术能定期接受国家科技委员会内相关部门的检查，查看其是否与国土安全和网络空间安全的要求相符，以及是否与联邦研究日程相符。

### 优先事务III：国家网络安全意识和培训计划

**A/R 3-1:** 国土安全部将与相关的联邦、州和地方实体以及私营部门相协调合作，推动全面的网络安全意识培养行动，其内容包括针对特定对象制定相应的培训教材，扩大“安全在线”（StaySafeOnLine）活动，面向工业界中为安全做出突出贡献的人员制定奖励项目。

**A/R 3-2:** 国土安全部将和教育部一起，在合理的预算下，鼓励并支持州、地方和私营组织制定针对中小学生学习网络安全学习的项目和指南。

**A/R 3-3:** 家庭用户和小型商业机构可以通过保护自己的网络连接的安全以帮助提高国家网络空间的安全。个人或企业的计算机操作人员可以通过安装并定期更新防火墙软件、安装最新的杀毒软件、定期更新操作系统和应用程序以增强系统的安全性，这将有助于增强网络空间的安全性。为促进用户采取这些保护措施，国土安全部将组建一个由私营公司、组织和消费者群组成的工作组，通过该工作组，信息技术产品和服务的提供商或其他组织可以找到使家庭用户和小型商业机构更易于保护其系统安全的方法。

**A/R 3-4:** 鼓励大型机构对影响国家关键基础设施安全的内部网络的安全性进行评估。评估内容包括：（1）审计最佳实践措施的有效性及其应用；（2）制定连续性计划，考虑配备冗余人员和设备；（3）参与工业界范畴内的信息共享及对最佳实践措施的传播。

**A/R 3-5:** 鼓励各个学院和高校采取以下全部或部分安全措施来加强其网络系统的安全：（1）建设一个或多个 ISAC，以处理网络攻击和网络脆弱性问题；（2）制定相关政策，授权首席信息官处理网络安全问题；（3）为 IT 安全制定最佳实践措施；（3）制定模范的用户安全意

识项目和教材。

**A/R 3-6:** 持续的公共-私营合作联盟将有助于通过以下工作来保护国家网络基础设施的安全：在必要和可行时参与对技术和研发的缺陷分析，从而能够对联邦的网络安全研究日程提供输入，对相关的研究进行协调，并制定和传播网络安全的最佳实践措施。

**A/R 3-7:** 国土安全部将实施并鼓励在美国国内制定用以推动网络安全专业培训的项目，包括与国家科学基金会（NSF）、人事管理办公室（OPM）和国家安全局（NSA）相协调，一起探寻如何利用现有的“网络警察服务奖学金”项目以及由《网络安全研究和开发法》创建的为各类研究生、博士后、高级研究人员和教员提供的奖学金和受训项目。

**A/R 3-8:** 国土安全部将与具有网络安全培训知识的其他机构相协调，一起制定一种协调机制，将联邦政府的网络安全培训与计算机司法取证培训项目联系起来。

**A/R 3-9:** 国土安全部将鼓励为建设一个公私部门广泛认可的安全认证项目而开展必需的基础工作。国土安全部和其他联邦机构将有效而清晰地描述联邦 IT 安全界的需求，以协助这些工作的开展。

#### **优先事务IV：保护政府部门的网络安全**

**A/R 4-1:** 联邦机构将继续扩大对自动化的安全评估和安全策略实施工具的使用，并积极部署威胁管理工具，从而能够检测到攻击。联邦政府将判断是否必须采取特定的措施（通过政策或财政预算流程）来促使各个机构更多地使用这些工具。

**A/R 4-2:** 通过现在正在实施的电子鉴别活动，联邦政府将审查对强访问控制和身份鉴别的需求，研究联邦各部使用相同的物理和逻辑访问控制工具及鉴别机制的范围，最终进一步推动一致性和互操作性。

**A/R 4-3:** 联邦机构应当考虑安装能持续检测非授权网络连接的系统，各个机构的政策和流程应当反映出对风险消减措施的考虑，包括使用强加密技术、双向鉴别、防辐射标准及技术、配置管理、入侵检测、事件处理、计算机安全意识与培训项目。

**A/R 4-4:** 联邦政府将对国家信息保障联盟（NIAP）重新进行全面的考查，以判断其对商用软件产品不断出现的安全缺陷这一问题的解决程度。这一考查过程将吸取在实施国防部 2002 年 7 月发布的政策时得到的教训。该政策要求产品在采购时应经过 NIAP 或类似评估流程的审查。

**A/R 4-5:** 联邦政府将考虑是否有必要对联邦政府的安全服务提供商进行认证，以考查其是否具有最小的能力，包括考查其是否具有足够的独立性。

**A/R 4-6:** 鼓励州和地方政府为其各个部门和机构制定 IT 安全项目，包括意识培养、审计及标准；鼓励各州与其他情况类似的州一起参加已经建立的 ISAC。

#### **优先事务V：国家安全和国际网络安全合作**

**A/R 5-1:** 联邦调查局和中央情报局应当确保以更强有力的反情报姿态来打击针对美国政府、商业和教育机构的以网络空间为基础的情报收集行为。这项工作必须包括要更加深入地了解我们的对手利用网络空间进行间谍活动的能力和意图。

**A/R 5-2:** 情报部门、国防部和执法机构必须增强迅速调查攻击源的能力，以便于及时有效地做出响应。与国家安全战略一致，这些工作同样将努力发展相关能力来抵抗对关键系统和基础设施的攻击。

**A/R 5-3:** 美国必须增强与网络攻击和间谍活动有关的执法部门、国家安全部门和国防部

门之间的协调能力，确保各个部门之间在适当情况下能够互相交换与犯罪事件相关的信息。国家安全委员会和国土安全办公室将对此进行研究，以确保相应的协调机制到位。

**A/R 5-4:** 当某个国家、恐怖主义集团或者其他敌人通过网络空间攻击美国时，美国政府的回应不需要局限于对犯罪活动进行起诉。美国保留以适当的方式进行回应的权力，美国将为这类意外事件做好准备。

**A/R 5-5:** 美国政府将通过适当的国际组织加强合作，与企业建立合作联盟，以推动国外公共-私营部门间就信息基础设施保护展开对话，并推动全球“安全文化”的形成。

**A/R 5-6:** 美国将与加拿大和墨西哥合作，将北美打造成“安全的网络空间地带”。我们将会把该项目扩展到标识和保护那些用来支撑电信、能源、运输、银行与金融系统、应急服务、食品、公众健康和供水系统的关键公共网络。

**A/R 5-7:** 美国将督促每个国家在处理千年虫问题的经验基础上为国内和国际之间的网络安全工作指定集中化的联系地址。这些联系地址的建立能够极大地增强国际协作能力以及对问题的解决。我们还将督促每个国家都建立自己的观察和预警网络，用于向政府部门、公众和其他国家对可能发生的攻击或病毒发出通知。

**A/R 5-8:** 为了促进在出现网络威胁时的实时信息共享，美国将支持建立能够接收、评估和发布此类信息的全球网络。该网络可由 FIRST 之类的非政府机构负责建设。

**A/R 5-9:** 美国政府鼓励区域性组织，如 APEC、EU 和 OAS 等，分别建立或指派负责网络安全事务的委员会。这类委员会也可以通过与来自私营部门的代表共同建立联合工作组受益。美国政府还鼓励区域性组织，如 APEC、EU 和 OAS 等，与来自政府和私营部门的代表建立网络安全事务联合委员会。

**A/R 5-10:** 美国将鼓励其他国家接受《欧洲委员会网络犯罪公约》，或确保其法律和流程至少包含了相关内容。

---

## 七、关键基础设施和重要资产的物理保护 国家战略

美国白宫

2002 年 7 月

---

我的美国同胞们：

2001年9月11日的恐怖袭击表明，面对恐怖主义威胁我们脆弱到了何种程度。然而在悲剧事件发生之后，我们作为一个团结的国家，展示了保护关键基础设施和重要资产不被恐怖分子进一步利用的坚定决心。在这一努力过程中，各级政府、私营部门和全国公民竭诚合作，采取了统一的行动。

为了抵御企图危害美国的威胁，关键基础设施的所有者和运营者开始评估关键基础设施的脆弱性并加大了对安全的投入。全国各州及城市政府在各自辖区内继续采取重要措施确保对重要资产和服务的保护。在不断加强及时交流重要安全信息的同时，联邦各部门和机构还与工业界紧密合作，协调了关键性资产和设施的保护行动。国土安全办公室正在与各大公共-私营部门实体密切合作，以建立覆盖各级政府和关键性部门的国土安全顾问系统。最后，我对国会议员们在国土安全部立法中的辛勤劳动表示赞许，这部法律将把国家关键基础设施和重要资产的保护工作统一到即将设立的国土安全部的领导之下。

但是，要长期坚持这些初步努力，我们仍有很多工作要做。这部《关键基础设施和重要资产的物理保护国家战略》只是日后长远征程的第一个里程碑，该文件与《国土安全国家战略》一脉相承，确定了一系列明确目标和目的，概述了加强对于公共卫生和公众安全、国家安全、政府运作、经济稳定和公众信心来说至关重要的基础设施和资产保护的指导方针。它提供了一个统一的框架，说明了责任和义务，确定了近期开展重点保护工作的重要方案。最为重要的是，它为政府、工业界和社会公众共同保护我们的关键基础设施和资产的合作环境打下了一个基础。

《关键基础设施和重要资产的物理保护国家战略》是几个月来征询广大公共-私营部门利益相关人意见的产物。这份文件采纳了联邦部门和机构、州和城市政府、私营部门基础设施所有者和运营者、科学技术团体、专业协会、研究机构和全国相关人士的广泛建议。这一文件题为国家战略，堪称名至实归。

在实施本国家战略的过程中，牢记保护关键基础设施和重要资产是所有人的共同责任这一点至关重要。因此，我们的保护工作成功与否，取决于各级政府与私营部门的紧密合作。我们每个人都在保护基础设施和资产的工作中扮演着重要角色，而这些基础设施和资产是我们日常生活的基础，代表着我们的国家实力和国家声望。

我们所面对的恐怖主义敌人有着坚定的信念、极强的耐力和适应性。在这样的威胁之下，保护关键基础设施和重要资产称得上是一项巨大挑战。我们必须全国上下同心协力，以强有力的措施和协调一致的行动来克服这一挑战，保护我们的国家和我们的生活方式。

——布什

## 1. 执行摘要

本文阐明了《国土安全国家战略》提出的一个核心任务领域——通过保护关键基础设施和重要资产减轻国家面对恐怖主义活动的脆弱性所必须经由的道路。

《关键基础设施和重要资产的物理保护国家战略》（以下简称“本战略”）确定了一系列明确目标和目的，概述了加强对于公共卫生和公众安全、国家安全、政府运作、经济稳定和公众

信心来说至关重要的基础设施和资产保护的指导方针。它还提供了一个统一的框架，确定了近期开展重点保护工作和调整资源配置的具体方案。最为重要的是，它为政府、工业界和社会公众各行其责，共同保护我们的关键基础设施和资产的合作环境打下了基础。

本战略认识到，作为对 2001 年 9 月 11 日事件的反应，全国的公共和私营实体采取了很多重要措施来改善其关键设施、系统和功能的安全状况。在这些努力的基础上，本文为在关键基础设施和重要资产保护中起重要作用的联邦部门和机构指明了方向。它同时还对州和地方政府、私营部门实体和全美各地相关人士提出了所应采取的措施，用以加强我们共同的基础设施和资产的安全。从这个角度看，本战略属于并适用于整个国家，而绝非仅仅针对联邦政府及其组成部门和机构。

### 新任务

“9·11”事件表明，我们的国家在恐怖主义集中强大力量实施大规模破坏的威胁面前有多么脆弱。这一天发生的事件同时还证明，我们的恐怖主义敌人在制定和执行计划上多么有决心和耐心，手段有多么狡猾。我们自由社会的基本特性极大地方便了恐怖分子的行动和策略，同时也阻碍了我们预防、阻止或减轻恐怖活动造成危害的能力。基于这些事实，在全国范围内实施全面物理保护势在必行。

### 确定终极战略目标

加强国家关键基础设施和重要资产保护的战略目标包括：

- 确定和稳妥保护关系到全国公共卫生和公众安全、政府运作、经济稳定、国家安全以及公众信心的关键基础设施和资产。
- 及时发出警报，确保面临迫近的具体威胁的基础设施和资产得到保护。
- 制定具体方案并建立一个合作环境，使联邦、州、地方政府和私营部门得以更加有效和效率更高地保护由他们控制的基础设施和资产，从而确保有可能成为恐怖分子长期攻击目标的其他基础设施和资产安全无恙。

### 国土安全和基础设施保护：共同的责任

保护美国关键基础设施和重要资产的任务要求我们转而采用一种全新的全国合作方式。国土安全的基本原则与历史沿袭的国家安全原则有着根本性差别。从传统意义上说，国家安全主要是联邦政府的责任。国家安全是通过保卫我们的领空和国家边境的军队、外交人员和情报人员的共同努力以及保护我们的国家利益的海外行动实现的。

国土安全，特别是对关键基础设施和重要资产的保护，则是全体民众的共同责任，不可能由联邦政府独当一面。它需要联邦、州和地方政府、私营部门以及全国相关人士采取协调一致的行动<sup>①</sup>。

---

① 《国土安全国家战略》将“州”定义为“美国的任何州、哥伦比亚特区、波多黎各、维尔京群岛、关岛、美属萨摩亚群岛、美属北马里亚纳群岛或太平洋群岛托管地”。本战略将“地方政府”定义为“任何县、市、村、镇、行政区或其他任何州的下属政治分区、美国土著部族或授权的部族组织或阿拉斯加州土著村庄或组织，其中包括任何乡村社区或未自治的镇或村，或其他任何由州或下属政治分区申请国家资助的公共实体”。



## 行动案例

要想制定和实施一项稳健的战略来保护我们的关键基础设施和重要资产并防止这些关键基础设施和重要资产被恐怖分子进一步利用，我们就必须了解敌人的动机以及他们惯用的伎俩和目标。同时，我们还必须综合评估需要得到保护的基础设施和资产、它们的脆弱性以及消除或减轻脆弱性所要面临的挑战，后者是需要全国上下共同做出努力方能完成的任务。

### （1）关键基础设施的重要性

美国的关键基础设施部门为国家安全、政府运作、经济活力和生活方式提供了基础。而且，这些关键基础设施的可靠性、安全性和可恢复性给人民以信心，从而成为我们的国家特征和国家意志的重要组成部分。关键基础设施支撑了我们的日常生活，使我们得以享受世界上最高的一种生活标准。

构成关键基础设施的设备、系统和功能种类繁多，十分复杂。它们包括人力资产以及在运行过程中高度相互依赖的物理和网络系统，还包括在关键基础设施发挥功能的运行中十分重要的关键节点。

### （2）重要资产的重要性

重要资产和重大活动是单个的攻击目标。这样的资产如果遭到攻击，在最糟的情况下，不仅会导致大规模人员伤亡和财产损失，而且还会影响我们国家的声誉、士气和自信心。

单个而言，核电站和水坝之类的重要资产对于国家级关键服务的连续性或许并不十分重要。但是对这些目标的成功袭击，除了从长远来看会对公共卫生和公众安全不利之外，也许还会导致人员和财产的重大损失。另外，还有一些重要资产则象征着美国传统的价值观和制度或者美国的政治和经济力量。我们的国家标志性建筑物、纪念碑和历史遗迹珍藏了我们的历史和光荣成就，表现了我们国家的庄严伟大。它们代表着美国人民的理想和生活方式，因此也是恐怖分子垂涎的攻击目标，特别是当有重大庆祝活动在那里举行并且有大量人群聚集的时候。

### （3）了解威胁

#### ①恐怖主义的特征

发生在世贸中心和五角大楼的“9·11”事件反映了恐怖主义敌人的决心。他们持续几年以世贸中心塔楼为目标，表明了恐怖分子的残酷无情和坚韧耐心。恐怖分子也是机会主义的，灵活性很强。他们从经验中汲取教训，避强就弱，不断修改自己策略和攻击目标。随着越来越多的可预料目标加强了安全措施，他们将目标转移到保护力量薄弱的资产。因此，针对恐怖分子的具体策略或目标采取对策，很有可能会迫使恐怖分子转而采用其他策略。

#### ②可能的攻击特性

恐怖分子追求的长期战略目标包括对关键基础设施和重要资产的攻击。恐怖分子以关键基础设施为目标发起的攻击大体上是为了造成以下三种后果：

- 直接影响基础设施：通过对某一关键节点、系统或功能的直接攻击，连锁性破坏或阻碍关键基础设施或重要资产发挥功能。
- 间接影响基础设施：通过公共和私营部门对攻击的反应，给政府、社会和经济带来连锁性破坏和经济损失。
- 利用基础设施：利用某一个基础设施的元素破坏或摧毁另一目标。

## 国家政策和指导方针

本战略重申了有关关键基础设施和重要资产保护的长期国家政策。它同时还提出了行将支撑国内保护战略的一系列指导方针。

### (1) 国家政策综述

作为一个民族，我们有责任全力保护我们的关键基础设施和重要资产，以防恐怖活动会：

- 削弱联邦政府执行重要国家和国土安全任务和确保普通公共卫生和公众安全的能力；
- 破坏州和地方政府维护法令和提供最低限重要公共服务的能力；
- 破坏私营部门确保经济有序运作和提供重要服务的能力；
- 削弱公众的士气以及对国家经济和政治制度的信心；

我们必须齐心协力，利用必要的工具保护我们的关键基础设施和重要资产。

### (2) 指导方针

本战略共有八项指导方针：

- 保障公众安全、公众信心和各项服务；
- 明确责任和义务；
- 鼓励和推动各级政府之间以及政府与工业界之间建立合作伙伴关系；
- 鼓励推出可能的市场解决方案并通过政府集中干预弥补市场紊乱造成的损失；
- 促进有意义的信息共享；
- 加强国际合作；
- 开发以抵御恐怖分子威胁的技术和专业技能；
- 保护个人隐私和宪法所保障的自由。

## 通过有组织的合作来保护关键基础设施和重要资产

本战略的实施需要有统一的组织、明确的目的、对角色、责任和义务的深入了解以及一系列被普遍接受的合作流程。可靠的组织计划可以推动各级公共和私营部门有效参与和相互合作。没有这样的计划，协调和整合国内保护政策、制定规划、配置资源、评估业绩以及实施向联邦、州、地方政府和私营部门授权的方案的任务就不可能完成。我们的行动战略必须对这些实体提供其赖以支撑的基础，使它们得以运用必要的核心力量、专业技术和经验应对迫在眉睫的威胁，实现协调一致的目标。

### (1) 联邦政府的责任

联邦政府具有广泛组织、召集和协调其管辖权限内政府机构和私营部门的能力。它有责任制定连贯的政策和战略以及执行这些政策和战略的实施计划。在国土安全方面，联邦政府将协调政府和私营机构的补充性努力和能力，以提高我们长期保护每个关键基础设施和重要资产的水平。

每次恐怖事件都会对国家产生潜在影响。因此，联邦政府将在确保实现本战略《介绍》详述的三大主要目标的过程中发挥领导作用。这一领导责任涉及：

- 密切关注我们最关键的设施、系统和功能，督促经济部门和政府机构做好防范准备。
- 确保联邦、州、地方政府和私营实体携手合作，共同保护面临威胁和 / 或其损失会对国家造成重大影响的关键设备、系统和功能。
- 及时对州、地方政府和私营部门合作伙伴提供并协调与之相关且具有行动意义的国家

级威胁信息、威胁评估和威胁警报。

- 制定并执行全面的多级保护政策和计划。
- 探索各种潜在激励选择方案，以鼓励利益相关人遇到特殊保护问题时自行开发解决方案。
- 开发跨部门、跨辖区的保护标准、指南、规范和协议。
- 促进关键基础设施和重要资产保护最佳处理方式、实践流程和脆弱性评估方法的共享。
- 进行试验性项目和计划示范演示。
- 促进先进技术的开发和转让，利用私营部门的专业技能优势。
- 在全国范围内开展关键基础设施和重要资产保护教育，提高全民保护意识。
- 提高联邦政府与州、地方政府以及服务供应商合作的能力。

#### (2) 联邦领导部门和机构

《国土安全国家战略》为关键基础设施和重要资产保护提出了一个基于部门的组织框架。它指出联邦领导部门和机构有责任协调保护活动，有责任发展和维护与州、地方政府以及关键部门工业机构之间的合作关系。

除了确保联邦政府拥有和运营的基础设施和资产的安全以外，联邦领导部门和机构还应在以下方面对州、地方政府和私营部门合作伙伴提供帮助：

- 组织和实施保护工作，保持操作计划的连贯性，提高对关键设施、系统和功能脆弱性及其所受威胁的了解和认识。
- 验证和推广具体部门行之有效且高效率的保护手段和方法。
- 扩大部门内各私营实体之间及政府与私营实体之间有关安全信息的自愿共享。

#### (3) 国土安全部

在这个新的组织规划中，作为联邦机构、州和地方政府以及私营部门之间合作主要联络人和推动人，国土安全部将负责对跨部门保护工作做全面协调。致力于跨部门协调的国土安全部还将负责具体修订和实施本战略核心部分的工作。

#### (4) 其他联邦部门和机构

除了指定的联邦部门和机构外，联邦政府还将依靠其他部门和机构独有的专业技术来加强对国土安全的保护力度。此外，适合于所有部门的全面方案一般会包含国际成分和需要，这要求发展与其他国家政府或机构的协调关系，同时要求与外国政府共享信息。因此，国务院将通过为与我们的盟国达成双边和多边基础设施保护协议打下基础，来支持部门保护方案的制定和执行。

#### (5) 州和地方政府的责任

作为我们国家组成部分的 50 个州、4 个托管领地和 87 000 个地方辖区在保护关键基础设施和重要资产的工作中起着重要且独特的作用。与联邦政府相同，州和地方政府也应该确定并保护其在辖区内拥有和运行的关键基础设施和重要资产。

州政府还应通过与指定的联邦领导部门和机构密切合作，在本辖区和地区协调保护行动、应急响应行动和资源支持。州政府应该深入协调关键基础设施和重要资产保护的规划和准备工作，运用统一标准确定设施和资产的关键性，确保保护的重点投资，规范辖区内的防范工作。当面临的威胁超出辖区和辖区内实体的能力时，州政府还应疏通寻求联邦政府协助的渠道。最后，州政府还应该推动安全信息和威胁警报的交流下达到地方政府一级。

当需求超出了地方政府的能力时，州和地方政府可以寻求联邦政府进行协调、提供支持和

资源。关键基础设施和重要资产的保护需要各级政府间的广泛合作。国土安全部的设立，尤其是为了在包括关键基础设施和重要资产保护在内的国土安全问题上协调州和地方政府的工作。其他联邦领导部门、机构和执法机关将在具体保护关键基础设施和重要资产时提供必要和适当的支持。

#### （6）私营部门的责任

我们的关键基础设施和重要资产主要由私营部门拥有和运营。私营部门的公司制定风险管理计划时往往十分慎重，同时把对安全的投资看作是商业运作和树立用户信心的必备功能。此外，在当前威胁丛生的环境中，私营部门通常把守着保护自身设施的第一道防线。因此，私营部门基础设施的所有者和运营者应该对自己的规划、担保和投资方案重新进行评估和调整，以便更好地适应由恶意暴力行为带来的日益增长的风险。自“9·11”事件以来，为了适应新的危险环境，很多企业增加了限度投资并加强了安全保卫工作。就大多数企业而言，对安全的投资水平反映了隐含风险与后果之间的平衡，这一平衡基于：（1）对风险环境的了解；（2）在经济上合理、在竞争激烈的市场中或在政府资源有限的环境中得以生存的要素。如果说恐怖主义威胁的动态特性以及后果的严重性与潜在的攻击谋划相关，那么私营部门自然会寻求从政府得到信息，以帮助它们更好地做出关键基础设施安全投资决策。

同样，当私营部门面临的威胁超出了企业的自我保护能力、超越了合理的附加投资水平时，它们也会寻求政府提供帮助。鉴于此，联邦政府应该与私营部门（以及州和地方政府）密切合作，确保国家级关键基础设施和资产的安全；及时发出警报，确保面临迫在眉睫具体威胁的关键基础设施和资产得到保护；创造一个能使私营部门在其中更好地履行具体保护责任的环境。

#### （7）近期蓝图：跨部门的安全重点

本文《跨部门的安全重点》一章概述的问题和安全方案是近期需要优先考虑的国家重点。它们集中体现在关键基础设施和重要资产保护所遇到的阻碍上，而这些阻碍会对政府、社会和经济多个部门产生巨大影响。针对这些得到确认的问题的潜在解决方案，如信息共享、威胁提示和警报等，具有杠杆的推动作用，一旦得以实施，我们国家保护全国关键基础设施和重要资产的能力将会得到整体提升。因此，国土安全部以及被指定的联邦领导部门和机构将会实施周密计划，以支持这章阐明的各种行动。

本战略从以下五个方面提出了跨部门的重点方案。

##### ①计划和配置资源。本战略在这个方面提出了八个重点方案。

- 为政府和工业的关键基础设施和重要资产的保护计划创建合作机制。
- 确定需要保护的关键重点并为其开发适宜的支持机制。
- 在公共和私营部门之间促进风险管理专业技能的共享。
- 为积极采取安全强化措施的私营机构确定方案选项。
- 协调和巩固联邦政府和州政府的保护计划。
- 建立一支队伍，负责对关键基础设施或重要资产遭到攻击后的重建和恢复工作所遇到的法律障碍进行分析研究。
- 建立一个完整的关键基础设施和重要资产地理空间数据库。
- 与我们的国际伙伴共同制定关键基础设施保护规划。

##### ②信息共享、迹象发现和预警。本战略在这个方面提出了六个重点方案。

- 定义与保护相关的信息共享需求，建立行之有效且高效率的信息共享流程。

- 行使 2002 年《国土安全法》赋予的法定权威和权力，保护私营部门的敏感安全信息和私有信息。
- 促进关键部门信息共享和分析中心的发展和运作。
- 改进国内威胁数据的采集、分析和发布流程，使其能够达到州和地方政府以及私营行业一级。
- 支持州和地方政府以及被指定的私营部门实体开发公用的安全通信系统。
- 全面实施国土安全顾问系统。

③人员的可靠性、建立人力资产和提高人员认识。本战略在这个方面提出了六个重点方案。

- 协调人员可靠性国家标准的开发。
- 为进行人员背景筛选工作的公司制定认证计划。
- 为私营部门安全官员开发一种认证制度或样板式安全培训计划。
- 确定需求和制定保护重要人员的计划。
- 促进公共和私营部门之间共享用于保护的专业技术。
- 为关键基础设施和重要资产保护制定和实施一项在全国范围内提高公众认识的计划。

④技术研发。本战略在这个方面提出了四个重点方案。

- 协调公共和私营部门的安全研发活动。
- 协调公用标准以确保通信系统的兼容性。
- 开发识别和鉴别人员身份的方法。
- 提高技术监督、监控和检测的能力。

⑤建模、仿真和分析。本战略在这个方面提出了七个重点方案。

- 把建模、仿真和分析整体融合到国家基础设施和资产保护计划和决策性支持活动之中。
- 开发能够应对恐怖主义攻击的短期和长期影响的经济模式。
- 发展关键节点 / 阻塞点和互依赖性分析的能力。
- 根据部门预警流程和行动之间的冲突模拟各部门的互依赖性。
- 就网络 and 物理威胁、脆弱性和后果建立综合风险模型。
- 开发能够提高信息完整性的模型。

### 特殊的保护域

除了本战略提出的跨部门问题外，具体的基础设施部门和特殊类别的重要资产也存在很多问题需要采取行动。相关的考虑和方案将在本战略的最后两章中讨论。

#### (1) 保护关键基础设施

本战略针对以下关键基础设施部门提出了重点保护方案：

- 农业和食品；
- 水资源；
- 医疗卫生；
- 应急服务；
- 国防工业基地；
- 电信；
- 能源；

- 运输；
- 银行与金融；
- 化学工业和危险原料；
- 邮政和递送。

(2) 保护重要资产

本战略针对以下类别重要资产提出了重点保护方案：

- 国家纪念碑和标志性建筑物；
- 核电站；
- 水坝；
- 政府设施；
- 商业重要资产。

## 2. 介绍

2002 年 7 月 16 日，布什总统颁布了《国土安全国家战略》。这是一部动员和组织整个国家保护美国本土安全以防恐怖主义攻击的全面战略。它传达了一个“基于与国会、州和地方政府、私营部门及美国人民共同承担责任并通力合作的原则”的全面方案。这项工作确实需要举国上下同心协力，绝不是联邦政府单独所能应付的。

《国土安全国家战略》定义了“国土安全”，提出了一个基于三个国家目标的战略框架。这三个国家目标按优先次序是：（1）阻止恐怖分子在美国境内的攻击；（2）减轻美国面对恐怖活动的脆弱性；（3）将所发生的攻击造成的损失和恢复代价降至最低。

为了达到这些目标，《国土安全国家战略》把我们的国土安全工作分列了六个关键领域：情报和预警、边境和运输安全、国内的反恐活动，保护关键基础设施和重要资产、防范灾难性恐怖活动以及能源防范和响应。

《关键基础设施和重要资产的物理保护国家战略》（以下简称“本战略”）<sup>①</sup>为《国土安全国家战略》提出的一个核心任务领域（通过保护关键基础设施和重要资产减轻国家面对恐怖活动的脆弱性）推动了制定战略规划的过程。它确定了一系列明确的国家目标和目的，概述了加强对于公共卫生和公众安全、国家安全、政府运作、经济稳定和公众信心来说至关重要的基础设施和资产保护的指导方针。它还提供了一个统一的框架，确定了近期开展重点保护工作和调整资源配置的具体方案。最为重要的是，它为政府、工业界和公众各行其责、共同保护我们的关键基础设施和资产的合作环境打下了一个基础。

本战略认识到，作为对 2001 年 9 月 11 日世贸中心和五角大楼遭受攻击事件的反应，全国的公共和私营实体采取了很多重要措施以改善其关键设施、系统和功能的安全状况。在这些努力的基础上，本战略为在关键基础设施和重要资产保护中起重要作用的联邦部门和机构指明了方向。它同时还对州和地方政府、私营部门实体和全美各地相关人士提出了所应采取的措施，用以加强我们共同的基础设施和资产的安全。从这个角度看，本战略属于并适用于整个国家，

---

① 本战略的重点是关键基础设施和重要资产的物理保护。有关具体部门的信息技术和网络资产的保护战略，《保护网络空间的国家战略》中进行了详细论述。因此，信息和电信部门的信息技术设施保护在本文中并没有涉及。

而绝非仅仅针对联邦政府及其组成部门和机构。

本战略是《保护网络空间的国家战略》的补充。后者侧重于互联信息系统和网络的识别、评估和保护。物理保护战略和网络保护战略有着共同的根本性政策目标和原则，它们一起构成了通向国土安全核心任务领域之一的道路。

### 新任务

发生在世贸中心和五角大楼的“9·11”事件表明，我们的国家在恐怖主义集中强大力量实施大规模破坏的威胁面前有多么脆弱。这天发生的事件同时还证明，我们的恐怖主义敌人在制定和执行计划上多么有决心和耐心、手段有多么狡猾。具有讽刺意味的是，我们自由社会的基本特征极大地方便了恐怖分子的行动和策略，同时也阻碍了我们预防、阻止或减轻恐怖活动造成危害的能力。基于这些事实，在全国范围内实施全面物理保护势在必行。

保护美国的关键基础设施和重要资产是一项重大挑战。我们国家的关键基础设施和重要资产涉及错综复杂、种类繁多且相互依赖的设备、系统和功能，面对各种各样的威胁显得非常脆弱。巨大的数量、广泛的分布以及高度互联的性质，使它们成为恐怖分子可以得到无限回报的攻击目标。潜在目标的庞大规模和广泛范围，使我们不可能随时对它们施以全面保护，令其免受任何可能的威胁。当我们为某一类目标设计保护措施时，我们的恐怖主义敌人很可能正聚焦在另一类目标上。要想取得更佳效果，我们的国家保护战略就必须建立在全面了解这些复杂性的基础上，唯有如此，我们才能制定和实施重点突出的行动计划。

### 确定终极战略目标

要想勾勒出国家保护工作的初步重点框架，我们就必须认识到，作为基础设施部门组成成分的资产、系统和功能并非一律都是“关键”的，从全国或主要地区的角度看尤其如此。

本战略的**第一大目标**是确定并稳妥保护那些我们认为对于国家级公共卫生和公众安全、政府运作、经济和国家稳定以及公众信心至为“关键”的资产、系统和功能。我们必须对国家级关键性设施、系统和功能进行重点分明的综合评估，同时对各基础设施部门防范工作实施监控。联邦政府将与州和地方政府及私营部门密切合作，建立确定国家级关键性的统一方法。这种方法将侧重于开展重点活动和开发抵御恐怖主义威胁的一致措施。

本战略的**第二大目标**是确保面临具体威胁的基础设施和资产的保护工作得以顺利实施。联邦、州和地方政府及私营部门必须密切合作，开发全面评估和预警的流程和系统，以确保受威胁资产及时得到预先警告。这些实体必须进一步合作，以集中力量应对预料中的威胁。

最后，我们在保护关键基础设施和资产时还必须认识到，关键性是随时间、风险和市场的变化而不断演变的。为了更好地保护最重要的设备、系统和功能，我们应该能够预计到，恐怖主义敌人也会把他们破坏的目标转移到在他们看来保护措施比较薄弱、更有可能产生预期打击后果的地方。因此，本战略的**第三大目标**是通过各方合作的措施和方案确保其他那些有可能随着时间的推移而吸引敌人动心的潜在目标。本战略的侧重点是为主要公共和私营部门的利益相关人创造一个环境，使他们得以在其中根据各自的责任、资格和能力更好地保护他们控制的基础设施和资产。

本战略的最后三章详述了我们行将施行的跨部门以及针对具体部门的重点解决方案，目的是使所有类别的关键基础设施和重要资产都能得到最完善的国家级保护。

## 国土安全和基础设施保护：共同的责任

美国关键基础设施和重要资产的保护要求出现一种全国上下通力合作的全新转变。国土安全与历史上定义的国家安全在基本原则上是完全不同的。历史上，保护美国需要向境外派遣军队。我们通过地理意义上的“保护邻近地区的安全”来保护我们自己。执行这种任务的能力和责任感大都归属于联邦政府。

国际恐怖主义在我们境内的出现，使国内安全的警戒线移到了美国本土地区。面对“9·11”事件，现在的保护国土任务需要真正意义上的“保护邻近地区安全”。保卫祖国以防恐怖主义威胁需要我们恰当配置和使用内在资源。我们社会的开放性和多样性、全体公民的个人权利和自由以及我们政府的联邦制度，决定了实施安全保卫的框架结构。

联邦政府如果单独行动，它必然缺乏对国土安全威胁做出反应和实施有效保护所必需的综合工具和能力。因此，为了抵御恐怖主义对我们的关键基础设施和重要资产的威胁，我们必须充分利用与我们处于同一新战线的实体——地方机构及组成国家关键基础设施部门的私营部门实体的资源和力量。

这种史无前例的合作的形成，需要彻底改变冷战时期形成的心态。这方面的努力必须取得成功，而且还要长时间保持下去。本战略为如何实现这一全国范围合作提供了一个起始点。

对于这种堪称典范的新型全国合作，本战略将进一步起重要作用，将就紧迫的恐怖主义威胁以及政府和工业界在保护工作中应该承担什么责任对公众进行宣传教育并努力实现现实的预期。公众对本战略的理解和接受至关重要。只有预期清晰明了并且能够实现，美国公众的回应和支持才能即便在遭受恐怖主义攻击后也能长期保持。

## 本战略简述

本战略涵盖范围广大而又注重细节。以下各章为更全面地保护我们的关键基础设施和重要资产应该采取哪些具体的重点行动勾勒出一幅蓝图。

### （1）情况分析

本章论述了关键基础设施和重要资产作为国家经济稳定、政府运作、国防、公共卫生和公众安全以及公众信心的基础所扮演的角色。它详细阐明了恐怖主义的特征以及我们为保护国家关键基础设施和重要资产免受威胁所要面临的挑战。

### （2）国家政策和指导方针

本章阐述了支持本战略的国家政策和指导方针以及我们通过合作实施的行动方案。

### （3）通过有组织的合作保护关键基础设施和重要资产

本章为我们的国家级关键基础设施和重要资产保护工作提出了一个组织结构。它还阐明了重要公共和私营部门的作用和责任，并为跨部门、跨辖区的基础设施和资产保护提供了一个合作框架。

### （4）跨部门的安全重点

本章阐述了关键性的跨部门问题、行动的障碍以及克服障碍的步骤。它介绍了加强合作、降低成本和通过杠杆推动关键问题领域取得最大效果所需采取的行动。这些方案也构成了一个框架，使我们得以在其中将联邦预算的资源配置到关键基础设施和重要资产的保护任务中。

### （5）关键基础设施保护

本章概述了《国土安全国家战略》确认的关键基础设施部门的保护重点。这方面的综述旨



在突出各部门需要重点关注的紧迫问题。每个联邦领导部门和机构都将制定相应的规划和计划，帮助实施或改进这些重点部门方案。

#### (6) 重要资产保护

本章概述了水坝、核电站、国家纪念碑和标志性建筑物等特有设施的保护事宜。这些设施如果在最糟糕的情况下遭到攻击，会对公众的健康和安全 / 或公众的信心造成重大影响。

#### (7) 总结

本章总结了全面确保关键基础设施和重要资产安全所需采取的步骤。

### 3. 行动案例

为关键基础设施和重要资产保护制定一项行之有效的战略，要求对我们面临的威胁以及这些威胁的潜在后果有清醒的认识。“9·11”事件为我们敲响了警钟。在这些灾难性事件发生之前，美国人认为我们相对强大的力量可以使国土免受大规模攻击。我们在冷战中取得的胜利，使我们几乎没有面对过传统意义上的重大军事威胁，世界恐怖主义看来在中东之类的麻烦地区比在中美洲更值得关注。作为一个民族，我们一般不了解恐怖分子的动机以及隐含在他们计划背后的深仇大恨。更有甚者，我们低估了他们能量的深度和广度，完全预料不到他们的破坏会带来多么可怕的后果。“9·11”事件令我们猛醒，推翻了所有这些错误认识。

基地组织恐怖分子把我们的运输基础设施的关键元素作为武器。他们的目标是象征着我们国家威望以及军事和经济力量的重要资产。攻击的后果一泻千里，殃及了我们的社会、经济和政府。作为一个民族，猛然之间我们痛苦地意识到，我们国家的民主制度居然是这样的脆弱，这种感受比第二次世界大战后的任何时代都要强烈。

为了保护我们的关键基础设施和重要资产免受恐怖分子进一步利用，我们必须了解恐怖主义行动的意图和目标，以及他们为攻击各种目标而采用的策略和技术。我们必须通过对需要保护的资产、它们的脆弱性以及减轻或消除这些脆弱性所要面临的挑战进行全面评估来加深这一了解，而减轻或消除这些脆弱性是一项需要整个国家共同做出努力方能完成的任务。

#### 关键基础设施和重要资产的重要性

##### (1) 关键基础设施的重要性

美国的关键基础设施部门为我们强大的国防和繁荣的经济提供了必要的物资和服务。而且，它们持续保持的可靠性、活力和可恢复性铸造了一种自信的氛围，成为我们国家身份和战略目标的重要组成部分。它们还构成了我们的生活方式，使美国人民能够享受高于世界上任何国家的生活标准。

打开电灯开关，我们马上能够见到光明；拿起电话听筒，我们马上能够听到拨号音。拧开水龙头，我们马上能够用到清澈的水；电、净水和电信只是关键基础设施所提供服务中的一小部分，我们把这些服务看作是理所当然的。它们已经成为我们日常生活最基本的要素，以至于只有当这些服务由于某些原因而中断时，我们才会注意到它们。每当出现服务中断的情况，我们都期望得到合理的解释，并希望能服务能够尽快恢复。

《国土安全国家战略》把我们的关键基础设施分为以下几个部门：农业、食品、供水、医疗卫生、应急服务、政府、国防工业基地、信息和电信、能源、运输、银行与金融、化学工业和危险原料、邮政和递送。

这些工业提供了：

①基本物资和服务的生产和交付

农业、食品、供水等关键基础设施部门与医疗卫生和应急服务一起，为美国人民提供了其赖以生存的重要物资和服务。

能源、运输、银行与金融服务、化工产品制造、邮政服务和邮件递送维系着国家的经济并使物资和服务的整体供应得以继。

②相互连接和可操作性

信息和电信基础设施连接并越来越有力地控制着其他关键基础设施的运作。

③公共安全和稳定

我们的政府制度确保了我国国家的安定、自由、运转以及构成国家公众安全网络的各项服务。

构成我们关键基础设施的设备、系统和功能种类繁多，十分复杂。它们包括人力资产以及在运行过程中高度相互依赖的物理和网络系统，还包括了在关键基础设施发挥功能的运行中十分重要的关键节点。更为复杂的是，我们的大部分关键基础设施通常都是互联的，因此需要依赖其他动态系统和功能的持续正常运行。

例如，电子商务要依赖电力、信息与通信；而电力供应服务又要求运输和配送系统正常运行，以确保发电所需燃料的供应。这样的互依赖性已经存在很久了，是对前所未有的大规模消耗效率和生产力的运营流程进行革新的产物。由于这些相互依赖的基础设施具有动态性质以及我们日常生活对基础设施高度依赖，破坏或摧毁它们的成功恐怖攻击，其巨大影响会远远超出受直接攻击目标本身，并且会在直接破坏发生后的很长一段时间内持续存在。

(2) 重要资产的重要性

重要资产系指这样一些个体目标，它们如果遭到破坏，会造成大规模人员伤亡或财产损失，同时还会使我们国家的声誉和信心受到严重打击。仅就这样的资产和活动本身而言，它们并不是确保全国范围重要服务持续性的关键要素，但是它们当中的任何一个如果遭到攻击，在最坏情况下，都会造成重大人员伤亡和 / 或公共卫生和公众安全的损失。这类重要资产包括核电站、水坝和危险原料存储仓库等设施。

其他类型的重要资产具有象征意义，代表着美国的传统价值观和制度或美国的政治和经济力量。我们的国家象征、标志性建筑物、纪念碑和历史遗迹珍藏了我们的历史和光荣成就，表现了我们国家的庄严伟大。它们代表着美国人民的理想和生活方式，因此也是恐怖分子垂涎的攻击目标，特别是当有重大庆祝活动在那里举行并且有大量人群聚集的时候。

重要资产的所属关系差异很大。私营部门拥有并运营着水坝、核电站以及国内大部分具有重要商业价值或象征意义或者有大量人群家居或工作的大型建筑。国家纪念碑和标志性建筑物的保护往往重叠归属于州、地方和联邦政府。有些则靠私营基金会管理和运作。这些事实使我们的保护工作变得更加复杂。

## 了解威胁

(1) 恐怖主义的特征

“9·11”事件不可否认地说明，我们的关键基础设施和重要资产已经成为恐怖主义极具价值的目标。这次攻击表明了恐怖主义的决心和耐心。多次打击的高度协调一致证明敌人在计划和实施阴谋方面极其狡诈，这是我们以前不曾预料到的。这些攻击表现出了基地组织恐怖分子追求目标的顽强决心。1993年，他们袭击世贸中心塔楼的第一次企图失败了，8年以后，他们

继续计划和实施第二次攻击，这次攻击的成功超出了他们的预期。

我们的恐怖主义敌人证实他们是机会主义的，灵活性很强。从对世贸中心的两次攻击中不难看出，他们从经验中汲取教训，避强就弱，不断修改自己策略和攻击目标。随着越来越多的可预料目标加强了安全措施，他们将目标转移到保护力量薄弱的资产。因此，针对恐怖分子的具体策略或目标采取对策，很有可能会迫使恐怖分子转而采用其他策略。

恐怖分子不仅在选择攻击目标方面足智多谋，在选择和使用具体暴力工具方面也同样如此。他们一旦发现薄弱环节，马上就会选择时间和地点不择手段地加以利用。恐怖分子想方设法获取武器，其中从威力巨大的传统炸药和轻武器到大规模杀伤武器，称得上应有尽有。他们通常根据目标的特点决定使用什么武器，有些时候则根据所使用的特定类型武器，如核武器或生化武器，来决定攻击什么目标。方法和目的的匹配只受恐怖分子的创造性和资源限制。唯一不变的是，他们在追求战略目标时，希望造成最大程度的破坏、伤亡和动荡。

恐怖主义在未来的一段时间内还会存在。“9·11”事件后布什总统指出，与恐怖主义的斗争将是一个漫长的过程。恐怖分子的工具和策略会改变，但他们的基本决心是不变的。那些对美国及美国的利益心存敌意的人把恐怖活动视为对付我们的一大有力武器，只有到我们拿出证据证明对付恐怖主义已经不在话下的时候，他们才会放弃幻想。

## （2）可能的攻击的性质

恐怖主义与我们的较量涉及政治、经济和心理等多方面的目标。恐怖分子为了达到他们的目的，可能会把攻击关键基础设施和重要资产选作风险较低的手段，企图以此造成大规模人员伤亡、动荡和恐慌。

恐怖分子把目标锁定在关键基础设施和重要资产上是为了达到以下三种目的。

- 对基础设施直接产生影响：通过对关键节点、系统或功能的直接攻击，连锁性破坏或阻碍关键基础设施或重要资产的运行。

对金融服务部门重要资产密布的世贸中心塔楼实施攻击，立竿见影地破坏了这些设施并造成服务中断，这是对基础设施直接产生影响的例子。

- 对基础设施间接产生影响：通过公共和私营部门对攻击的反应，给政府、社会和经济造成连锁性破坏和带来经济后果。

“9·11”事件造成公众不愿乘飞机旅行和其他经济问题，是这种影响的例子。要想减轻这类攻击带来的严重后果，需要对政策和对策进行认真评估，了解攻击会给公众造成什么心理影响，恰当权衡对小规模攻击采取具体行动的利弊。

- 利用基础设施：利用某个基础设施的元素来破坏另一目标。

在“9·11”事件中，恐怖分子利用航空基础设施攻击世贸中心和五角大楼这两个美国经济和军事力量的中心。确定这类攻击造成的连锁性跨部门潜在后果极其困难。

## 保护关键基础设施和重要资产面临的挑战

### 新的前线

我们的科技高度发达的社会和制度其实就是恐怖分子大有可乘之机的潜在攻击目标。我们的关键基础设施工业为适应作为其服务对象的市场的需要而高速地变化着。规划及实施关键基础设施和重要资产保护所必需的很多专门技术从没有被联邦政府采用过，其中不乏如何准确确定哪些设施和资产必须得到保护的专业技术。实际上，在这场新型战斗中，防护工作的第一线

已经转移到了我们的社区以及构成我们关键基础设施部门的机构个体中。

私营行业拥有并运行着大约 85% 的关键基础设施和重要资产。设施的运营者一直在履行保护自己的物理资产免受未经授权外来者入侵的职责。然而这些措施在传统意义上无论多么有效，一般都不是专为应对重大军事和恐怖主义威胁或者由这些威胁造成的连锁性经济和心理影响而设计的。

关键基础设施和重要资产的独有特征、它们的持续快速发展以及使保护工作复杂化的各种重大障碍，要求关键性公共和私营部门携起手来，进行史无前例的合作和协调。我们的国家仅地方政府辖区就有 87 000 多个。我们面临的挑战是要建立一种能够加强保护力度，而不仅是完全模仿的相互协调和相互补充的系统，这个系统还要适应合作者相互间的重要需求。此外，我们很多关键基础设施是跨越国界的，因此保护工作还离不开国际合作的基础。

### 新的范例：合作和伙伴关系

开放的社会、极富创造性和反应迅速的经济市场以及形成自我认知和个人自由的价值体系，为我们的国家创造了财富，建立了强有力的国家安全系统，为未来灌输了一种民族自信心。破坏我们的传统、价值观和生活方式是恐怖主义的主要目标。具有讽刺意味的是，使我们得以充分享受自由的美国社会原则，也为恐怖分子的活动创造了方便的环境。

当我们努力了解恐怖主义的性质、寻找对付他们的适当方法的时候，我们需要有一套用以携手作战的新型合作结构与机制。冷战时期，很多政府和私营机构将他们的部分物理和信息基础设施孤立起来，形成所谓的“大礼帽”以确保安全。现在再用这样的办法来保护我们的国土免受意志坚定的恐怖分子攻击已经无法奏效了。要想激励举国上下自觉开展快速适应当前形势的保护行动，就离不开公共-私营部门相关人员的相互信任与密切合作，而绝不能再使用传统的命令和控制了。

“9·11”事件以后，各级政府和私营部门都增加了对安全的投入。恐怖主义日渐猖狂，我们只有这样做才能保护我们的国家和我们自己。保护工作要求各级政府和私营部门付出高昂的成本，其中包括开发新技术、新工具和新方案所需的开销。因此，行之有效的保护战略必须与由国家精英们通过信息创新和共享、最佳实践措施和共享的资源开发出来的规划周密、高度协调的方法相结合。

### 国家的恢复能力：长期持续的保护工作

对抗恐怖主义是一场旷日持久的斗争。恐怖主义的动态特性意味着我们必须在威胁长期存在、不断发展的环境下加强对我们的关键基础设施和重要资产的保护。

一般而言，我们国家的关键基础设施生机盎然，具有很强的恢复能力。这些特性得自于几十年来抵御飓风、洪水之类自然灾害以及居心不良者的恶意行动的经验。关键基础设施部门从每次破坏中总结教训，将其运用到日后的保护、反应和恢复工作之中。例如，“9·11”事件发生后，纽约的电力系统在曼哈顿除世贸中心爆炸发生地点以外的其他地区依然工作正常。而且，当世贸中心爆炸地点需要时，这里的电力服务很快就恢复了，有力地支持了营救和恢复工作。这是体现美国人才智的一个极好例子，是 1993 年世贸中心爆炸和其他恐怖事件经验教训的成功应用。

恢复能力是美国大多数社区的特征，这一特征体现在人民与自然灾害的斗争中。随着时间的推移，连续遭受自然灾害地区的居民把握了灾情发生时的情况。这些地区的公共机构和居民

逐渐了解了灾难的性质，也懂得自己在处理灾难后果时应承担哪些责任和义务。他们还熟悉并依靠赢得了信赖的社区系统以及用以支持保护、反应和恢复工作的资源。因此，他们对于自己所在社区与处理灾情和从灾害事件中吸取教训的能力充满了信心。

全国的各种机构和居民也必须像这样逐渐了解恐怖主义的性质、其所带来的后果以及自己在与恐怖主义的斗争中所应承担的责任。从理想的角度而言，他们应熟悉并信赖自己所在社区现有的保护、反应和恢复机制。私营机构和居民必须与地方政府携手合作，不断改善这些系统和资源，以保护我们的国家免受恐怖主义攻击。

我们面临的挑战是总结、理解并应用“9·11”事件的教训，保护我们的关键基础设施和重要资产，预防其未来遭受恐怖分子攻击。我们的能力将决定我们对现有危险环境的适应程度，决定我们能否在不改变自己的价值观和生活方式的条件下成为一个更加强大、更加兴旺的国家。

保护工作面临的挑战见下表：

农业和食品	1 912 000 个农场，87 000 个食品加工厂
供水	18 000 个联邦水库，16 000 个城市废水处理设施
医疗卫生	5 800 家注册医院
应急服务	87 000 个美国本土地点
国防工业基地	215 个行业中的 250 000 家企业
电信	20 亿英里电缆
能源	2 800 家电厂 300 000 个生产基地
电力	
石油和天然气	
运输	5 000 个机场 120 000 英里主要铁路线 590 000 座高速公路桥梁 200 万英里管道 300 个内陆 / 海岸港口 500 个主要城市公共运输运营者
航空	
客运铁路	
高速公路、卡车运输和客车运输	
管道	
海运	
公共运输	
银行与金融	26 600 家联邦储蓄保险公司投保机构
化学工业和危险原料	66 000 家化工厂
邮政和递送	1.37 亿个配送站点
重要资产	5 800 座历史建筑物 104 家商用核电站 80 000 座水坝 3 000 个政府拥有或运营的设施 460 座摩天大厦
国家纪念碑和标志性建筑物	
核电站	
水坝	
政府设施	
商业资产	

## 4. 国家政策和指导方针

### 国家政策综述

本文重申了有关关键基础设施和重要资产保护的长期国家政策，同时还阐述了一系列巩固关键基础设施和重要资产保护国家战略的指导方针。

作为一个民族，我们有责任全力保护我们的关键基础设施和重要资产，以防恐怖活动：

- 削弱联邦政府执行重要国家和国土安全任务和确保普通公共卫生和公众安全的能力；
- 破坏州和地方政府维护法令和提供最低限重要公共服务的能力；
- 破坏私营部门确保经济有序运作和提供重要服务的能力；
- 削弱公众的士气以及对国家经济和政治制度的信心。
- 利用必要的工具保护我们的关键基础设施和重要资产。

作为一个民族，我们必须齐心协力，运用一切可用工具，制定和实施政策包含的各项保护措施。本文“介绍”中提出的战略目标将侧重于推动这方面的工作。

### 指导方针

我们的国内保护工作所基于的是核心力量和价值观基础，在历史上，我们的国家就是依靠这些力量和价值观渡过重大危机的。以这些核心力量和价值观为前导，以下八条原则突出了本战略的核心内容以及与之相关的行动方案。

#### （1）保障公众安全、公众信心和各项服务

恐怖分子企图通过大规模破坏摧毁公众对政治经济制度的信心，所以他们会不断对人身和财产使用暴力手段，以此来阻挠社会和经济的有效运行。不断从战略角度强化安全措施、减轻国家关键基础设施和重要资产面对物理攻击（尤其是那些可能造成灾难性后果的攻击）的脆弱性，这样的策略就是寻求增强公众对我们的制度和系统的信心。

有计划地对我们的关键基础设施和重要资产采取备份、固化和分散配置等措施，可以增强它们的生命力和抗攻击能力，从而不至于面临攻击时蒙受重大损失。通过行之有效的保护和反应计划，可使关键基础设施和重要资产快速恢复关键性服务，从而把攻击对我们的经济和社会安定的影响降到最低。实施精心制定的计划可以确保关键基础设施和重要资产在危机发生时正常运转，这是树立公众希望和增强公众对国家处理恐怖袭击后果能力的信心的关键所在。

#### （2）明确责任和义务

本战略阐明了政府、工业界和全体公民在关键基础设施和重要资产保护工作中的重要作用。我们联邦制度的宝贵遗产和有限的政府资源下放管理职权，赋予了社会公民和私营机构以一定的权利和自由过自己喜欢的生活和从事商业活动。在这样的背景下，不归联邦政府直辖的组织和个体就必须在关键基础设施和重要资产保护的很多方面担负起领导责任。

因此，本战略的一个重要组成部分就是阐明对国内保护工作起重要作用的各种公共和私营部门实体的责任和义务。这其中必然包含了涉及联邦、州和地方政府以及私营部门的必要的协调机制、综合性保护政策、规划、资源管理、业绩度量和行动方案。

### （3）鼓励和推动各级政府之间以及政府与工业界之间的合作

保护关键基础设施和重要资产涉及各级政府和私营部门。长期的保护工作必然是我们共同的责任，需要在全国范围内集中资源和专门技术。《国土安全国家战略》阐明了动员整个社会共同保护我们的国土的必要性。因此，它着重强调“州和地方政府、私营部门和美国人民都要发挥重要作用”。这一原则对于我们保护关键基础设施和重要资产至关重要。每次破坏活动或攻击最初都只是局部问题。地方社区、州和地方政府、私营部门基础设施所有者和运营者受到的直接影响，总是形成对恐怖袭击的主导性反应。因此，公众的信心依赖于社区执行保护措施和预先制定的保护计划的力度。鉴于此，联邦政府将就此提供总体支持、协调和集中领导，以建立一个能使所利益相关人都能更好履行自己的保护职责的环境。

### （4）鼓励推出可能的市场解决方案并通过政府集中干预弥补市场紊乱造成的损失

保护我们国家的关键基础设施和重要资产要求采取涉及范围极广的可行行动，其中包括提高对当前受威胁环境的了解和认识、提供威胁提示和警报、投资开展研发工作、推广实验性技术、探索各种财政刺激方式、在适当的地方采取目的明确的调整行动。

联邦政府将通过本战略大力推动具有前瞻性并基于市场的保护方案出台。很多关键基础设施部门目前已经调整到位，只有当市场力量不足以促进确保关键基础设施和重要资产保护工作正常进行所必需的投资时，才需要下达进一步调整的指示和命令。另外，当需要实施统一的国家标准或做出协调一致的反应以迎接特殊的挑战性威胁时，尤其是在各部门高度互依赖性的情况下，也需要下达进一步调整的指示和命令。

在很多情况下，财政刺激方案可以促使私营部门以及州和地方政府加强对情况的了解和提高它们的经验，其中包括适合于其具体系统、运营和安全挑战的新工具和创新性流程的开发。财政刺激方案还有助于抵消因市场情况变化而造成的某些负面影响，例如市场压力的自然趋势要求消除冗余性，从而造成市场紊乱。

### （5）促进有意义的信息共享

信息共享可以巩固真正的合作伙伴关系，同时是减轻狡猾、适应性强且意志坚定的敌人的威胁的必要条件。要想制定全面的安全计划，在了解多方面情况的条件下做出安全投资和行动决定，个人以及机构都需要及时、准确的相关信息。因此，我们必须采取措施确定和评估实施与安全相关的信息共享的障碍，并且制定适当的措施来克服这些障碍。我们还必须开发和发展可靠、安全、有效的通信和信息系统，以支持公共和私营部门实体之间有意义的信息共享。

### （6）加强国际合作

“9·11”事件以后，美国迅速联合世界各国的朋友和盟国发起了反恐战争。我们还迅速采取行动，与加拿大和墨西哥一起实施相关计划，旨在提高我们的共同边境以及跨境基础设施的安全水平。保护我们的关键基础设施和重要资产免受恐怖分子攻击，需要世界各国的进一步参与。在这个以相互依赖为特征的世界上，国际合作是我们保护计划的一个重要组成部分。

### （7）开发技术和专业技能以抵御恐怖分子的威胁

《国土安全国家战略》强调了科学技术的重要性，它们是国土安全的重要基础。关键基础设施和重要资产保护必须充分利用我们的科技优势，以使我们的保护工作效果更好、效率更高、付出的代价更低。共享国家资源、加强公共-私营部门之间的合作，将使最新的科学技术能够

得到充分利用，从而提高我们的保护工作抵御致命威胁的能力。

同样，建模、仿真和分析水平的不断提高可以增进我们对所必须加以保护的基础设施和重要资产复杂且相互依赖的性质的了解。这方面的应急响应能力将推动保护规划、决策和资源配置工作的开展。

#### （8）保护个人隐私和宪法保障的自由

我们的社会由多样化的种族、民族、文化、宗教和政治观点组成。这一多元化特征以及社会调和差异的能力，是美国强大实力的来源所在。但是，正如《国土安全国家战略》所指出的那样，我们的自由社会也有其固有的脆弱性。然而，公民权利和自由是我们国家特征的必要组成部分，这些自由和权利的任何损害都意味着恐怖分子的阴谋得逞。

因此，我们必须接受一定程度的恐怖主义风险会在我们的日常生活中长期存在这样一种现实。我们的任务是找出方法降低风险，并且在维持形成我们生活方式的自由权利的同时保护我们的国家。在全民共同实施安全保卫的同时，我们还要尊重个人隐私、言论自由、行动自由、免受非法歧视的自由以及使我们形成一个国家的其他珍贵的自由。

### 组织起来寻求伙伴共同保护关键基础设施和重要资产

执行全面的国家基础设施和重要资产保护战略，需要清晰统一的组织，明确的目的，对角色、责任和义务的透彻了解以及一整套深入人心的协调流程。一项结构严谨的组织方案可为公共-私营部门的积极参与和有效合作搭设一个舞台。没有这样的组织方案，将不可能完成协调和整合国家保护政策、规划、资源管理、业绩计量的任务，也不可能发挥联邦、州和地方政府以及私营部门的积极性。

总统颁布的《国土安全国家战略》提供了一个定义明确、结构统一的组织框架，本文将就这一问题进行进一步论述。本章阐明了公共-私营部门在关键基础设施和重要资产保护工作中的角色和责任。从根本上来说，关键基础设施和重要资产保护的成功，取决于我们能否有效利用每个利益相关人所独有的核心实力和资源。鉴于所需采取的保护行动涉及范围极广和高度复杂，同时涉及了大量实体，定义明确的权力、义务和协调流程将成为成功和持续发展的国家保护工作的基础。

#### （1）组织机构和合作伙伴面临的挑战

联邦、州和地方政府管辖范围的重叠以及我们关键基础设施和重要资产所有权结构的重叠，对于保护工作来说是一个重大挑战。相关实体的情况各异，它们对保护任务和责任的理解决程度也会不尽相同。此外，这些组织机构和个体代表了复杂多样的系统、运作机制和企业文化。每个机构要从事的保护工作涉及范围十分广泛，相互之间差异很大。最后，联邦、州和地方政府辖区保护权限的重叠程度也有很大的不同。成功执行本战略所涉范围极广的保护行动，需要建立一个统一的组织框架，在这个框架下允许发展互补合作关系并有效配置我们国家的保护资源。

#### （2）明确角色和责任

在我们政府的联邦制度下，联邦、州和地方政府以及私营行业扮演着各自不同的具体角色并行行使着特定的功能，这些角色和功能必须结合为一个整体才能确保保护工作的正常进行。另外，每个关键基础设施所有者和运营者拥有着独有的能力、专门技术和资源，把它们适当结合起来，便可以为全面保护国家贡献出力量。

##### ①联邦政府的责任

宪法为联邦政府规定了定义明确的基本责任。提供一般性国家防卫和提高整个国家的福祉就包括在其中。只有联邦政府能够动用军事、情报和外交资产来维护美国在境外的利益。更为



现实的情况是，联邦政府还在州和地方政府的支持下，一直领导着维护边境安全的工作。在防止恐怖分子进入美国国土方面，联邦政府可以动用几种其独有的工具，其中包括：军事、外交情报的收集，移民和入籍法规，边防、海关检查以及港口、机场的安全检查。

联邦政府的执法功能由可用以协调应对安全威胁和突发事件的多种司法手段以及允许跨越州界和国界缉拿罪犯的机制组成。此外，联邦机构还开展关键性研究工作，协调保护规划和突发事件处理工作，并且向州和地方当局提供物质和其他形式的支持。这些功能构成了阻止、预防、保护和应急响应的元素。

除了这些关键性服务和功能外，联邦政府还能跨越政府管辖权限和在私营部门内进行组织、召集和协调。因此它也有制定连贯的国家政策、战略和计划的责任。在国土安全方面，联邦政府将协调政府与私营机构的工作互补，以提高我们长期保护每处关键基础设施和重要资产的能力。

每次恐怖主义事件都会造成全国性影响。因此，联邦政府将发挥领导作用，确保实现本战略“介绍”提出的三项基本目标。这一领导角色涉及：

- 密切关注我们最关键的设施、系统和功能，督促经济部门和政府机构做好防范准备。
- 确保联邦、州、地方政府和私营实体携手合作，共同保护面临威胁和 / 或其损失会对国家造成重大影响的关键设备、系统和功能。
- 及时对州、地方政府和私营部门合作伙伴提供并协调与之相关且具有行动意义的国家级威胁信息、威胁评估和威胁警报。
- 制定并执行综合性多级保护政策和计划。
- 探索各种潜在激励选择方案，以鼓励利益相关人遇到特殊保护问题时自行开发解决方案。
- 开发跨部门、跨辖区的保护标准、指南、规范和协议。
- 促进关键基础设施和重要资产保护最佳处理方式、实践措施和脆弱性评估方法的共享。
- 进行试验性项目和计划示范演示。
- 促进先进技术的开发和转让，利用私营部门的专业技能优势。
- 在全国范围内开展关键基础设施和重要资产保护教育，提高全民的保护意识。
- 提高联邦政府与州、地方政府以及服务供应商合作的能力。

作为我们最珍贵的标志性建筑物和纪念碑等很多国家重要资产的管理者，同时作为执行关键性任务的设施的所有者和运营者，联邦政府还肩负着重大的直接保护责任。因此，联邦政府将采取适当步骤：

- 确定它自己的关键设施、系统和功能。
- 确定这些资产所依赖的关键节点。
- 评估相关的脆弱性。
- 以适当措施减轻脆弱性和保护由其控制的设施和资产。

#### **联邦领导部门和机构**

每个关键基础设施部门都面临着独有的安全挑战。《国土安全国家战略》为保护美国的关键基础设施和重要资产提出了一个基于部门的组织框架（参见“保护关键基础设施和重要资产的联邦组织”）。这一组织框架阐明了负责协调保护工作、推动相关部门长期合作的联邦领导部

门和机构。

除了确保联邦政府拥有和运营的基础设施和资产的安全以外，联邦领导部门和机构还应在以下方面对州、地方政府和私营部门合作伙伴提供帮助：

- 组织和实施保护工作，保持操作计划的连贯性，提高对关键设施、系统和功能脆弱性及其所受威胁的了解和认识。
- 验证和推广具体部门行之有效且高效率的保护手段和方法。
- 扩大部门内私营实体之间及政府与私营实体之间有关安全信息的自愿共享。

每个联邦政府领导部门或机构都将推选一个“部门联系人”，作为部门与政府之间的主要联络渠道。工业界的相应“部门联系人”将由联邦政府领导部门和机构指定，由其作为中间人，负责协调本部门关键设施和系统保护的规划和行动。

联邦政府将扩大这一公共-私营部门合作模式，将其作为我们行动战略的重要组成部分。因此，新近被《国土安全国家战略》确定的关键基础设施部门的联邦政府领导部门和机构将立即采取行动，指定部门联系人和协调员，以推动保护工作大力展开。这方面的工作还包括确定本部门内的重要设施、系统和功能以及推动部门制定保护计划。

### **国土安全部**

联邦领导部门和机构的组织模式为国家级保护协调和规划提供了一个重点突出的领导结构。新建立的国土安全部将通过跨部门总体协调大幅度提高这一模式的效力。国土安全部将在联邦部门和机构、州和地方政府以及私营部门之间扮演推动合作的主要联系人和推动者的角色。

作为跨部门的协调人，国土安全部还将负责详细修订和实施本战略的核心内容。本章所含内容包括了建立和维护对国家级关键资产、系统和功能的完全、及时和精确评估，同时对各关键基础设施部门的脆弱性和保护工作现状进行评估。国土安全部将利用这些信息评估威胁，为受威胁关键基础设施及时发出警报，同时设立“红色小组”审查各部门和政府辖区的防范工作。此外，国土安全部还将与其他联邦部门和机构、州和地方政府以及私营部门合作，确定并执行保护关键基础设施和重要资产的补充计划和协调流程。这一工作的有效起点，就是联邦领导部门和机构以及州和地方政府当前采用的那种应对自然灾害的合作方式。

除了跨部门协调之外，国土安全部还将对若干个部门实施联邦领导的职责，这些部门包括政府、应急响应、运输、邮政和递送以及信息和电信。

为了履行这些责任，国土安全部将：

通过制定和实施自己的开放、兼容和针对结果的计划，与州和地方政府以及私营部门建立合作伙伴关系。

- 积极创造机会，建立已被证明行之有效的合作模式。
- 确定并共享联邦政府的核心权限、职能和被选定的资源，以推动合作伙伴大力开展工作。
- 促进机构和部门之间的真诚交流。

### **国土安全办公室**

国土安全办公室将继续作为与国土安全（其中包括关键基础设施和重要资产保护任务领域）相关的跨部门政策问题总统主要政策顾问班底和协调机构行使职责。国土安全办公室的作用是建议并辅助总统，协调执行部门在美国境内对恐怖分子攻击的侦察、戒备、预防、保护、反应和恢复工作。国土安全办公室将和管理和预算办公室一起，整理并签署总统有关关键基础

设施和重要资产保护的预算提案。国土安全办公室在其现有权限下，还将同管理和预算办公室一起，确保其他联邦政府部门和机构的预算能够有效完成各自的保护任务。

负责国家关键基础设施和重要资产保护的联邦政府部门如下图所示：



### 其他联邦部门和机构

除了指定的联邦领导部门和机构之外，联邦政府还将综合其他众多部门和机构特有的专业技术和知识，用以扩大国土安全保卫的范围。例如，国家科学技术学院的国家标准和度量实验室将在制定关键基础设施和重要资产保护工作的标准方面起重要作用。这一角色的最近实例体现在 2001 年 PATRIOT 法、2002 年《加强边界安全和签证改革法》和《国家建筑安全小组法》所用的语言中。

涉及整个部门的全面方案往往包含国际成分，需要发展与外国政府或机构的协调关系，其中包含与外国政府的信息共享。因此，国务院将通过为与我们的国际朋友或盟友签订双边或多边基础设施保护协议进行铺垫工作来支持保护计划的制定和实施。国务院将以其领导美国对外政策以及支持其他联邦部门和机构计划和工作的独有职责，在推动我们关键基础设施和重要资

产重点保护项目发展方面发挥重要作用。

## ②州和地方政府的责任

作为我们国家组成部分的 50 个州、4 个托管领地和 87 000 个地方辖区在保护关键基础设施和重要资产工作中起着重要且独特的作用。美国所有的州和托管领地都设有国土安全联络办公室，负责管理其反恐和基础设施保护工作。此外，各州还有执法机关、国民警卫队单位和其他负责保护州内社区的重要服务部门。

与联邦政府相同，州和地方政府也应该确定并保护其在辖区内拥有和运行的关键基础设施和重要资产。州政府还应通过与指定的联邦领导部门和机构密切合作，在本辖区和地区协调保护行动、应急响应行动和资源支持。州政府应该深入协调关键基础设施和重要资产保护的规划和戒备工作，运用统一标准确定设施和资产的关键性，确保保护的重点投资，规范辖区内的防范工作。当面临的威胁超出辖区和辖区内实体的能力时，州政府还应疏通寻求联邦资助的渠道。州政府还应推动安全信息和威胁警报的交流下达到地方政府一级。

很多州彼此之间通过全国紧急事件管理人员协会、全国州长协会等各种机构以及确保相互支持的协议，建立了组织严密的关系。它们可以在相互协调的条件下，依靠共同努力实施地区性保护方案。回应“9·11”事件的经历已经证明，用于处理危机情况的相互协助协议以及其他类似的有效合作方案，能够有效统一各辖区和机构的计划和行动。

每次破坏或攻击最初都只是地方性问题。不论受到攻击的基础设施归谁拥有和运营，在事件的影响扩大到全国范围之前，都需要地方政府和社区当机立断采取措施，地方政府和社区必须担负行动的最初责任。

地方政府站在保护工作的最前线，代表着面向美国人民的公共服务水平。地方政府必须了解自己的社区、居民、地形以及赖以维护公共卫生、公众安全和社会秩序的现有关键性服务项目。各社区在地方政府领导下确保公众的安全、经济机会和生活质量。因此，公众信心起始与地方，依赖于社区怎样计划和保护他们的市民、应对紧急情况 and 从混乱中恢复秩序。如果地方政府成功地防止并减少人员和财产的损失，或者像纽约在“9·11”事件中那样，面对灾难目标明确、工作有效，那么既能证明它们的能力，也能加强公众的信心。所以，地方社区有责任让市民做好应对紧急事件的准备，还要担负起领导责任，制定并协调地方和地区计划，确保对居民和商业的保护。

当需求超出了地方政府的能力时，州和地方政府可以寻求联邦政府进行协调、提供支持和资源。关键基础设施和重要资产的保护需要各级政府间的广泛合作。国土安全部的设立，尤其是为了在包括关键基础设施和重要资产保护在内的国土安全问题上协调州和地方政府的工作。其他联邦领导部门、机构和执法机关将在具体保护关键基础设施和重要资产时提供必要和适当的支持。

## ③私营部门的责任

我们的关键基础设施和重要资产主要由私营部门拥有和运营。私营部门的公司制定风险管理计划时往往十分慎重，同时把对安全的投资看作是商业运作和树立用户信心的必备功能。此外，在当前威胁丛生的环境中，私营部门通常把守着保护自身设施的第一道防线。因此，私营部门基础设施的所有者和运营者应该对自己的规划、担保和投资方案重新进行评估和调整，以便更好地适应由恶意暴力行为带来的日益增长的风险。自“9·11”事件以来，为了适应新的危险环境，很多企业增加了限度投资并加强了安全保卫工作。

就大多数企业而言，对安全的投资水平反映了隐含风险与后果之间的平衡，这一平衡基于：①对风险环境的了解；②在经济上合理、在竞争激烈的市场中或在政府资源有限的环境中得以生存的要素。如果说恐怖主义威胁的动态特性以及后果的严重性与潜在的攻击阴谋相关，那么私营部门自然会寻求从政府得到信息，以帮助它们更好地做出关键基础设施安全投资决策。同样，当私营部门面临的威胁超出了企业的自我保护能力、超越了合理的附加投资水平时，它们也会寻求政府提供帮助。鉴于此，联邦政府应该与私营部门（以及州和地方政府）密切合作，确保国家级关键基础设施和资产的安全；及时发出警报，确保面临迫在眉睫具体威胁的基础设施和资产得到保护；创造一个能使私营部门在其中更好地履行具体保护责任的环境。

及时可信的信息以及相关专业技术的提供，再辅以通过内部获得的工具和最佳实践措施，可以鼓励私营部门提前在风险管理的各个层次上谨慎投资。通过建立互惠互利关系和协调一致开展保护工作，公共和私营部门的合作伙伴关系可以极大增强我们国家保护关键基础设施和重要资产的能力。

在与国土安全部以及其他联邦部门和机构合作的过程中，部门协调员将发挥关键性作用。部门协调员还将与政府人员共同确定、改进和推广面向具体工业部门的最佳实践措施。部门协调员将依靠国土安全部以及其他联邦政府领导部门和机构提供协调一致的指南、行业安全保卫标准以及对行动具有指导意义的预警，以此来实施自己的保护方案。私营部门可能还需要得到激励才能加大安全投资。因此，部门联络人和部门协调员应与政府的相关人员一起开发潜在的激励催化剂，同时扫除公共-私营部门合作的障碍。

除了政府的正式支持外，私营工业部门还可以用很多措施来在各个方面改善自己的安全状况。很多工业部门通过建立联盟来增加其运营的国家级关键基础设施的可靠性和确保公众对它们的信心。由于公众对某一部门总体业绩的看法能够影响股东对部门成员的评估，因此很多机构可以在一个框架内携手合作，共享与安全相关并具有可行性的最佳实践措施。由高度互联的业内企业组成的部门还达成了相互援助协议，以防一个系统遭到破坏对整个部门造成影响。能源部门（尤其是电力工业）保障可靠性的行动就是关键基础设施合作的一个实例。

早在“9·11”事件之前，就有若干个关键基础设施部门建立了信息共享和分析中心，以规范成员之间的信息交换和提高防范物理和网络破坏的运营风险的管理水平。此外，很多部门机构还与联邦政府的相应部门共同制定规划，对促进国家保护工作做出了贡献。联邦政府对部门信息共享和分析中心的支持和保护计划，现在必须扩大到新指定的关键基础设施部门。

合作伙伴关系将为制定和实施协调一致的保护战略打下基础。真正的合作伙伴关系需要不断的交流，其中最重要的因素是相互信任。但是目前，公共-私营部门之间建立这种合作关系尚存在障碍。当前人们采取的态度以及机构体系关系、操作流程和结构框架都是过去时代的产物。在当今市场高度流动和环境威胁丛生的条件下，要保护我们的关键基础设施和重要资产不受恐怖主义袭击，就需要一种新型的、更有利于合作的体系关系和态度。显然，合作伙伴是必不可少的。

## 5. 跨部门安全优先级

本章阐述了跨部门的全面安全保卫方案，体现了关键基础设施和重要资产保护工作的国家级重点，突出了那些需要立即引起注意、必须加强合作和提高安全投资成本效率的跨部门保护

问题和行动。下文所列保护方案还支持了本战略的三大根本性目标：（1）确定和确保我们国家最关键基础设施和资产的保护；（2）及时发出警报，确保基础设施和资产面临迫在眉睫的具体威胁时的安全；（3）创造一个能使所有利益相关人都能更好地保护其所控制的基础设施和资产的环境。

我们身处一个威胁丛生的环境，因此必须把安全视为核心实践措施和标准运营方式不可分割的组成部分，而绝不是处理其他问题时的附加问题。随着恐怖主义威胁的持续和发展，我们必须不断调整我们的安全计划和保护工作，以使它们得以长期有效运转。本战略后面提到的行动代表着我们国家在这一漫长行程中所要迈出的头几步。

本章阐述的跨部门安全重点可划分为以下几个类别：

- 规划和资源配置；
- 信息共享、迹象发现和预警；
- 确保人员可靠和建立人力资产；
- 技术研发；
- 建模、仿真和分析。

以下各节分别讨论了跨部门保护问题以及与该保护问题相关的障碍，随后阐明了迎接这些挑战和排除保护障碍所必须采取的具体行动。

### **规划和资源配置**

行之有效并且高效率的风险评估、保护规划和资源配置是密切相关的环节。它们取决于联邦、州、地方政府、私营部门以及我们的国际合作伙伴共同衔接和实现它们各自和共同的目标、需要和优先重点的能力。

州和地方政府的有限资源目前正面临着前所未有的需求。税收的减少意味着州和地方社区经常会缺乏足够的资源对关键基础设施实施全面保护。资源的匮乏要求联邦、州和地方政府必须更加有效地携手合作，对它们有限的资源进行评估、计划和配置。

工业界也同样要面对多变的威胁和困难的经济环境。在有些情况下，某些关键部门的企业把资源集中使用在维持贸易活动上。为了提高安全投资流程的稳定性，私营部门机构必须更加密切地协调关键基础设施保护计划，以确保联邦政府和州政府能够了解和认可它们未来的开支情况。

风险评估和风险管理也必须相互结合、相互调节。工业界和公共机构需要统一的词汇和标准来指导它们的保护工作。各级政府和私营部门在全国和国际层次上的密切合作是未来形成共同的语汇和观点的关键所在。

#### **（1）规划和资源配置面临的挑战**

对州和地方资源的大量需求、因缺乏协调而造成的不确定性以及恐怖主义威胁的多变性使国内保护环境面临着很多挑战。“9·11”事件以来，要求州和地方政府加强关键基础设施和重要资产、边境地区、机场和港口安全保卫的呼声越来越高。出乎预料的税收减少使很多州大受影响，对其在收支平衡条件下的工作能力提出了挑战。因此，州和地方政府无法在不相应削减其他项目和服务支出的条件下增加安全保卫措施的开支。

我们通常依靠州和地方政府来保护国家的重要资产（如桥梁、隧道、核电站、水坝、机场等）。而州和地方政府却往往需要联邦政府的资源来确保辖区内关键基础设施和重要资产的安

全。在威胁变化多端、愈演愈烈的情况下，决定以哪种最佳方式来合理和恰当配置归属于不同政府部门的有限资源，需要各级政府以前所未有的程度通力合作。

另一个资源配置挑战与各州申请联邦政府援助时所必须通过的机制有关。联邦政府的现行拨款审批政策和流程有时效率极低。由于州和地方政府官员必须根据不同的指导方针寻求从各种渠道得到资金，他们往往把遵守资金申请要求和审批流程视为导致工作重复的因素。改进现行机制、提高向州和地方政府提供联邦政府资金的效率，需要对联邦政府机构的问题进行全面考虑。

将美国各州和托管领地团结到关键基础设施保护的合作框架内，是另外一大挑战。州和地方政府执法机关和应急响应部门是防止恶意暴力行为的第一道防线。事实上，“9·11”事件以来，州和地方政府在全国范围内一直承担着大部分安全支出。我们的国家保护计划必须考虑它们关心的问题以及它们所受到的限制。

确定工作重点以加强基础设施保护的一大重要挑战，是估计恐怖袭击所可能造成的经济破坏十分困难。这种破坏既包括袭击的直接影响（如工厂和设备的损失），也包括随之而来的任何长期经济损失。随着时间的推移，连锁性后果往往会大大超过短期后果，但是对它们很难做出估计。对关键性商业运作的相对短期破坏有可能造成严重的经济滑坡（如价格波动、失去合同、失去资金、保险损失等）。精确预测这种影响的程度，需要对现代工业和金融市场体现出来的互依赖性有高度敏感。

在风险管理的过程中，关键性确定的某些方面也可能会造成意外后果。把某些设施指定为与国内保护工作相关的“关键基础设施”，有可能使对它们的安全和运作变得更困难并且开销更大。联邦政府必须与其他利益相关人共同采取协调一致的行动，开发出各种选择方案，以弥补因为当今这个威胁丛生的环境而所付出的代价。

统一各种不同的评估方法是另外一种挑战。目前，各部门和机构采用了各种各样的方法来对脆弱性进行评估。很多情况下，这些方法既不一致也互不兼容，从而使保护的整体规划和资源配置变得十分复杂。

很多关键基础设施还跨越了国境，这也提出了一项独特的挑战。因此，我们必须与全世界的朋友和盟国密切合作，共同制定相关计划，确保构成国际市场的相互紧密连接的基础设施的安全。

## （2）规划和资源配置方案

在规划和资源配置的过程中，联邦、州和地方政府以及私营部门的利益相关人有义务共同：

- 确定各自的关键基础设施和重要资产保护目标；
- 开展情况分析以确定增加安全投资的合理性；
- 制定安全底线、标准和指导方针；
- 针对并不自然存在于市场中的与安全相关的活动确定潜在方案。
- 为了实施这些行动，我们将实施以下活动。

### ①为公共和私营部门关键基础设施和重要资产保护规划建立合作机制

国土安全部以及其他联邦领导部门和机构将促进并鼓励发展定义明确的合作机制，使公共-私营部门可以通过这一机制在国家级保护规划和业绩测量方面展开合作。联邦政府还将与其他利益相关人共同评估关键基础设施和重要资产的脆弱性、共享信息、制定用以消除或减轻这些脆弱性的保护战略和计划以及制定袭击后恢复计划。国土安全部将就明确性、全面性、一致性

和资源配置重点对这些部门计划进行评估。

国土安全部将把各部门的单个计划综合为一个全面的关键基础设施和重要资产保护国家计划，同时公布与国家级保护行动相关的联邦政府年度计划、流程和预算。

#### ②确定关键保护重点并为这些重点建立适当的支持机制

国土安全部将与其他利益相关人共同制定一套统一的方法，用以保护具有国家级关键性的设施、系统和功能，帮助联邦、州和地方政府以及私营部门确定保护重点。国土安全部将通过这一方法建立一个综合数据库，将这些重要设施、系统和功能的相关信息分类存储。国土安全部还将对各关键部门的脆弱性和防范工作进行全面和不断更新的评估。这将有助于指导短期保护行动，并为长期的领导重心和根据情况进行资源投资奠定基础。

此外，国土安全部还将确定涉及多个年度的关键基础设施和重要资产保护方案，以使规划制定工作更具前瞻性、结构更合理。

#### ③加强公共和私营部门之间的风险管理技术共享

由于要求各异、标准不同，目前使用的风险评估方法也是千差万别。政府和工业界均可从对方的丰富经验中受益匪浅。国土安全部将协调历史教训和最佳实践措施的共享，以建立一个适合于不同使用者环境的国内保护评估框架。

#### ④为私营机构具有前瞻性地加强安全措施确定激励选择方案

在与私营部门协商的前提下，国土安全部将与商务部和财政部共同确定具有提高成本效益意义的适宜激励选择方案，以补偿利益相关人为加强安全而进行的投资。

这些方案包括奖励新政策的最早实施者，或者以财政刺激手段鼓励将安全强化措施结合到关键部门的产品和服务之中。

#### ⑤协调并巩固联邦和州政府的保护计划

国土安全部将与其他联邦政府部门和机构共同强化联邦保护计划，以明确角色、责任和预期。国土安全部还将与州政府共同协调保护规划工作，对州政府的行动提供明确指导。此外，国土安全顾问系统还将与州一级关键基础设施和重要资产保护计划协调一致。

⑥建立一个专家小组，分析研究关键基础设施和重要资产受袭后的重建和恢复工作会遇到哪些法律障碍

国土安全部将协同司法部召集联邦、州和地方政府以及私营部门的代表共同分析研究有可能阻碍紧急情况下恢复关键基础设施服务的法规和许可证审核流程，并寻找解决这些问题的方案。

关键基础设施的重建可能要求在紧急情况下必须放弃现有的法规和许可证审核流程。这些“事发后应急法规流程”的制定必须提前就被确定为公共和私营部门合作关系的一个组成部分。

#### ⑦建立一个完整的关键基础设施和重要资产地理空间数据库

为了使关键基础设施和重要资产保护的规划、分析和决策支持工作更加有效地进行，我们必须建立一个完整的关键基础设施和重要资产地理分布数据库，供联邦、州和地方政府以及私营部门访问和用于具体用途。

这方面的工作要求与政府相关部门和机构建立地理空间担保合作关系，由这些政府部门和机构充当图像/地理空间数据的代理人、合成人和协调人。国土安全部以及其他联邦部门和机构与私营部门合作，继续收集有关重点人口中心、国内关键基础设施部门以及跨国界基础设施的信息。这个数据库将为公共和私营部门高层决策者和运营规划者提供一个参考资料通用体系，从而得以对脆弱性分析、国内防范、突发事件管理等工作提供支持。



### ⑧与我们的国际伙伴共同实施关键基础设施保护计划

“9·11”事件以来，我们签署了多项了双边关键基础设施全面保护框架协议，并与我们的邻国加拿大和墨西哥共同实施了一系列保护方案。国土安全部将与国务院以及联邦其他部门和机构将扩大这一安全合作关系，以便我们的其他重要国际伙伴也加入进来。这方面工作的总体目标是确定我们的跨境基础设施的脆弱性以及消除或减轻这些脆弱性所需采取的措施。

### 信息共享、迹象发现和预警

要想应对与恐怖主义威胁相关的挑战，公共和私营部门关键基础设施和重要资产的利益相关人就必须能够密切合作。联邦政府，尤其是情报部门和执法机关在提供、协调和证实有关威胁的情报并将其通报给各级政府方面发挥着重要作用。同样，州和地方政府的执法机关和私营部门的安全实体也是地方威胁情报的无价来源。而且，它们比联邦政府更了解影响其设施、系统和功能的脆弱性。为与安全相关信息的交流和交换建立公认和有效的流程，是填补现存差距和奠定合作基础的关键所在。

交流安全信息所常遇到的困难是关键基础设施和重要资产保护工作发展的主要障碍。需要有超常的合作和坚定的信念才能改变这种状况。联邦、州和地方政府以及私营部门必须尽最大努力进行有效的信息共享，在最需要的部门之间建立起及时、有效、实用的交流通道。信息是与恐怖主义斗争的重要工具，给最需要的部门及时提供准确信息是安全保卫工作的重中之重。

恰当保护我们的关键基础设施和重要资产需要：

- 改进威胁情报的搜集工作；
- 对威胁进行全面评估和分析；
- 加强迹象发现和预警流程及系统；
- 完善信息共享活动的协调机制。

及时准确的信息是我们国家关键基础设施和重要资产保护工作的基础。这也是我们的保护战略的基础，唯有信息及时准确，我们的预防、警报、戒备和应急响应才能有效进行。目前，各级公共和私营部门之间的有效信息共享还存在着很大障碍。要克服这些障碍，我们必须：

- 明确交换安全信息的目的；
- 确定为达到这一目的而必须共享的信息类型；
- 确定如何及何时最适度共享并保护关键性安全信息；
- 确定这些信息的适宜接收者；
- 指定分析信息的责任并确定威胁的先兆；
- 信息分析工作完成并且明确了威胁先兆后，立即指定采取适当行动的责任。

#### (1) 信息共享、迹象发现和预警面临的挑战

政府各机构之间以及公共和私营部门之间信息共享活动的总体管理始终缺乏适当的协调和推动。因此，收集威胁信息、进行风险分析和发布警报的现有全国机制根本就不能满足国内保护任务的需要。

州、地方政府以及私营部门的官员指出，他们从联邦政府收到的威胁信息通常含混、重复，有时甚至互相矛盾。他们说，很少能收到有助于他们做出复杂的资源配置决策的具体、准确而且及时的警报。他们还说，即便在得到相关的及时信息时，也经常会由于安全审查方面的要求而无法将其下达到适当部门。

此外，现行的安全审查流程十分复杂而且代价昂贵，往往要拖很长时间。例如，现行规定要求有某些州和地方政府的执法官员接受两次审查，一次由州和地方政府进行，另一次由联邦政府进行。我们必须简化这一流程，提高它的效率，使之能够满足我们的保护需要。

事实上，保护国家关键基础设施和重要资产也许并不需要所有利益相关人都接受这样的审查。如果忽略情报来源和方法，很多情报报告或许已经称不上是机密文件。我们需要讲究时效的流程，用以对相关情报进行解密，或者将得自保密来源的信息进行筛选，将其传递给适当的接收者。这些问题由于敏感信息传递方式的低效以及现行确保所需信息适宜传递的机制而变得更加复杂了。目前，尚没有一个中央协调机制来评估敏感信息的影响和确保这些信息传送到需要它们的部门。除此之外，技术通信系统的缺乏也无法确保机密的威胁信息安全传输到基础设施的所有者和运营者手中。

上述问题提出了严峻挑战，阻碍了我们国家确保关键基础设施和重要资产安全所需合作关系的发展。其中最突出的是主要利益相关人之间缺乏信任，这是我们必须克服的问题。如果各种信息混乱不堪、相互矛盾，我们在反恐斗争中就会处于劣势。

## （2）信息共享、迹象发现和预警方案

2002 年《国土安全法》的制定表明，我们消除公共和私营部门之间信息共享障碍的工作中取得了实质性进展。该法规定，自愿提交国土安全部的关键基础设施信息，如附有特殊保护声明，将不受《信息自由法》和州的“阳光”法律的信息披露条款管辖。此外，如果这样的信息由可靠途径获得，未得提交人同意，将不能直接用于民事诉讼。

该法还规定政府必须建立接收、处理和保存自愿提交的关键基础设施信息以及保护这些信息保密性的流程。它还规定必须建立允许在联邦以及州和地方政府之间共享这些信息并对其保密的机制。该法授权联邦政府向相关商业机构、目标部门、其他政府机关和公众就关键基础设施所受潜在威胁提供咨询和警报。该法还规定，联邦政府必须保护构成警报来源的任何自愿的信息来源，同时还要保护有关信息所有者或其他不宜公开的信息。

最后，该法允许私营部门参与者之间自愿达成提高关键基础设施安全性的协议，其中涉及不存在承担反托拉斯法责任的适当形式的信息共享。在这种新法律制度下，国土安全部将可以向私营部门关键基础设施所有者和运营者保证，他们提供的敏感信息是有保密保障的。这些保证将鼓励私营部门与政府一起共享重要信息。同时，政府也将保证这样的行动不会减弱市场中的竞争。

建立一个更加有效的信息共享制度以完成我们的主要保护任务，需要政府进一步加强领导，同时需要公共和私营部门利益相关人之间的紧密合作。具体方案包括以下方面。

### ①定义信息共享要求，建立效果好且效率高的信息共享过程

我们首先必须采取的步骤之一，是准确定义与关键基础设施和重要资产保护任务相关的信息共享要求。这些要求应该侧重于实时威胁、脆弱性、突发事件数据、最佳实践措施、安全指南、风险评估和操作流程的共享。国土安全部将连同司法部、国务院和其他联邦领导部门和机构一起，领导这一与其他重要利益相关人（其中包括国际合作伙伴）建立双向要求框架的工作。一旦确定了这些要求，就必须建立相应流程，以确保适宜的使用者可以及时获取所需信息。

### ②行使 2002 年《国土安全法》规定的权力，保护被私营部门认为敏感和私有的信息

为了促进公共和私营部门之间有意义的信息交流，我们应迅速实施 2000 年《国土安全法》的规定，鼓励私营部门共享与安全相关的敏感信息和突发事件数据。因此，在该法建立的框架

内，国土安全部应与司法部、国会、其他联邦领导部门和机构以及各州的立法机关一起：

- 适当保护私营部门与政府共享脆弱性评估、突发事件报告和其他安全数据；
- 建立适当的机制，确保与我们的国际伙伴共享和交流与安全相关的信息。

### ③推动关键部门信息共享和分析中心的发展和运作

部门的信息分享分析和中心提供了一种公共-私营部门信息共享的模式，尤其是在提示和警报方面。很多关键基础设施部门都使用这种体系在本部门成员之间交流潜在风险、威胁、脆弱性和突发事件数据等信息。

信息共享分析和中心通常采用的运行机制可使各中心之间及时共享很多类别的相关敏感信息。信息共享和分析中心已被证实是一种成功的信息共享模式，但是它们的能力还可以进一步提高，尤其是在发展先进的分析能力方面。国土安全部和其他联邦领导部门和机构将进一步支持各部门通过信息共享和分析中心交流安全信息。同时，国土安全部将与工业界共同建立相应的流程和机制，以帮助推动州和地方政府参与信息共享和分析中心的运作。

### ④改善国内威胁数据的收集、分析和向州和地方政府及私营工业传送的流程

我们的情报机构拥有完善的收集、分析和发布威胁国家安全利益的信息的流程。我们必须建立类似的收集和评估流程，从而得以对来自各种渠道的有关国内关键基础设施和重要资产保护的信息进行综合分析。

我们还必须建立一些流程，以确保州和地方法执法机构以及关键基础设施和重要资产所有者和运营者能够充分和及时获得必要信息，其中包括对恐怖组织的策略、技术和流程的评估，对恐怖分子能力和动机的评估，其他国家反恐活动的经验教训，以及有关部门脆弱性的全面分析。

国土安全部将与情报机构和司法部共同开发全面收集、评估和发布威胁信息的流程，以综合提高情报和执法机构执行国内保护任务的能力。它们还将建立相关流程，以确保情报和执法数据的综合结果能够及时传达到利益相关人，其中包括开发对需要掌握这些信息的人员快速进行背景审查和发放安全许可证的方法。

### ⑤促进为州和地方政府以及指定的私营部门实体提供服务的安全通信系统的开发

国土安全部将召集国家标准计量局、国防部和其他相关机构的专家开发共享敏感信息的技术系统，进而帮助州和地方政府使用这一系统。

### ⑥完善国土安全顾问系统

国土安全顾问系统于 2002 年年初开始运行。国土安全部将继续与其他联邦政府部门和机构、州和地方政府以及私营部门一起，说明、协调和确定应对该系统所示涉及特定重要资产及其运行的各种级别威胁的行动。

## 确保人员可靠，建立人力资产并提高人员意识

国内安全工作要从我们的社区、我们的制度和我们的商业贸易开始。接触并操作我们的关键基础设施和重要资产的人员对于我们的国家保护计划至关重要。影响人员可靠性和建立人力资产的主要问题涉及以下四个主要方面。

- 制定安全措施，防止通敌雇员进行破坏活动或协助恐怖分子接近重要设施或系统。
- 培养和训练更多的熟练操作员和安全人员，以确保关键基础设施和重要资产的安全。
- 确保这些人员工作时的安全。
- 实施交流信息和提高人员认识计划，帮助企业和机构行动起来保护各自的资产并有效

控制风险。

#### (1) 人员的可靠性

“9·11”事件说明恐怖主义组织有能力打入美国社会长期潜伏伺机作乱。这种“内部人员威胁”日益成为各部门关键基础设施和重要资产保护工作的心头之患。“内部人员”是指那些能够正常接近重要设施和系统的雇员或其他人员，其中还包括承包商、临时聘用人员和外部供应商。这些内部人员能够自由出入和得到信任，往往会在有意或无意中泄露有关重要节点、脆弱性、操作特点或安全措施的信息，从而成为恐怖分子的帮凶。他们还可能直接为恐怖分子提供方便，使其接近运营中心和控制室之类的重要设施和系统。

#### (2) 建立人力资产

与人员可靠性密切相关的是确保可信、可靠、训练有素人员保护关键基础设施和重要资产免受恐怖主义攻击的基本需要。私营部门所有者和运营者要依靠技术娴熟的雇员来完成保护任务。安全人员，特别应急响应人员，需要得到足够的训练、装备和其他支持才能有效完成任务，此外他们在执行任务过程中还需要有一定的人身安全保证。

#### (3) 提高人员认识

常备不懈的状态要求广大社会公众，特别是在政府机构和最直接受影响的私营部门工作的人员，对我们面对的威胁的范围和性质以及我们所必须采取的预防措施有深刻认识。近年来，联邦政府与私营部门共同实施了一项系统计划，以提高关键部门重要企业领导人的保护意识。这项在“9·11”以后得到大力加强的工作已经取得了卓有成效的结果。此外，攻击涉及的范围以及由此引起的广泛宣传（如国会听证会和媒体的报道）也极大地提高了公众对恐怖主义威胁的认识。为了使我们国家的保护工作真正取得成功，这样的认识水平必须长期保持下去。

#### (4) 确保人员可靠、建立人力资产和提高人员意识所面临的挑战

对应聘者、访问者、固定和临时员工以及接触关键部位的承包商及时和定期进行全面背景审查，是预防“内部人员威胁”的重要手段。不幸的是，深入进行人员甄别和背景审查的工作往往超出了私营部门和非联邦政府机构的能力。私营雇主无法接触可帮助他们确定是否应该接纳雇员、承包商和来访者或者是否应该允许这些人接近敏感设施的人员可靠性资料（这些数据通常掌握在联邦政府手里）。兼职、临时和季节性员工流动性很大，对有效的背景甄别审查也是一大挑战。其他挑战还包括宪法规定的自由、审查流程的成本以及可证实的文件和其他信息来源的缺乏。

除了人员可靠性以外，各行业熟练员工（从安全技术人员到应急响应人员）的短缺也是保护关键基础设施和重要资产的严重障碍。同样，尽管私营部门安全人员是保护重要设备的重要力量，但是在整个关键部门，对于这些重要岗位却没有资格认定标准、培训或证书要求。鉴于恐怖主义威胁的动态特性，正在进行的安全人员培训急需保持技术水平，并根据恐怖分子武器和策略的发展而不断进行更新。

保护雇员免受恐怖分子威胁及袭击波及的潜在影响，是关键基础设施和重要资产所有者和运营者关注的重要问题。这也是雇员、安全人员和应急响应人员关注的重点。进一步的攻击有可能导致受害地区遭到生物、化学或放射污染，如果没有有效的预防措施，可能会威胁到应急响应人员及其家人（通过交叉感染）以及受攻击地区的其他人员。

尽管发生了“9·11”事件，工业界人士对恐怖主义威胁关键基础设施的严重性的认识依然处于较低水平。随着时间的推移，“9·11”事件在相关人士头脑中留下的印象渐渐淡去，普

通公众的认识和兴趣也一点点淡漠。因此，确保关键基础设施安全所必需的行动缺少了持续的重视，这使我们又一次暴露在了敌人的威胁之下。

(5) 确保人员可靠、建立人力资产和提高人员认识的方案

为了战胜这些挑战，我们将采取以下行动。

①协调制定人员可靠性国家标准的工作

国土安全部将与司法部共同组建一个顾问小组，对关键基础设施部门确保人员可靠性计划作全面分析研究。这个由联邦机构和部门、州和地方政府以及私营部门代表组成的顾问小组将就制定国家标准和建立背景审查、筛选以及对关键服务部门重要雇员进行识别的能力提出建议。

在各关键基础设施部门之间协调确保人员可靠政策和计划将有助于建立统一的标准。但是，在制定人员可靠性国家标准时，我们必须找到一个平衡点，使我们能够在降低风险并确保关键基础设施安全的同时维护个人自由。

②为进行人员背景审查的公司制定认证流程

为了补充私营部门的确保人员可靠性工作，国土安全部将和司法部共同为进行人员背景审查的公司建立一套认证流程，以确保能够对雇员的背景及时准确查证，并减少这个过程障碍。

此外，国土安全部将推动有关创建数据库或授权进入数据库识别选项的研究，以协助确定关键职位和其他潜在职位候选人以及合同工作人员和重要服务供应商人员的任用。由移民局以及其他各种情报部门和执法机关掌握的联邦数据库可以用来推动这种流程的建立。我们在这方面做出努力的同时，还必须谨慎从事，以保护由宪法保障的个人自由。

③建立私营部门安全官员认证制度或规范安全培训计划

为了最大程度地发挥美国私营部门安全人员的作用，国土安全部将与执法机构和联邦安全官员一起加强与州和地方政府相应部门、私营部门基础设施所有者和运营者以及专门从事私营安全官员培训和认证机制建立工作的私营安全公司之间的对话。由联邦执法学术机构制定安全人员培训计划是一种可行模式。

④确定重要人员保护需要并制定适宜计划

国土安全部将与州和地方政府以及工业界代表共同确定由于其在关键基础设施保护工作中的作用而有可能成为恐怖分子袭击目标的重要人员的保护需要并为此制定适当的保护计划。

必须确保安全人员和应急响应人员执行保护任务时的人身安全。需要给这些人员装备保护设备以及抵御有毒或生物污染的必要服装，同时也防止把潜在危险物质传播给他人。必须按计划确保安全人员和应急响应人员接受履行职责必需的保护训练和教育。

(6) 促进公共和私营部门保护技术的共享

国土安全部将与其他联邦领导部门共同促进公共-私营部门之间的保护技术共享。

培训和演练可起到检验保护计划和人员能力的作用，这对于共享最佳实践措施来说至关重要。因此，国土安全部将发展并综合现有方法，制定与保护关键基础设施和重要资产相关的培训计划，以达到解决一般性保护问题的目标。只要安排得当，这些方法都能适应公共和私营部门的培训和评估工作。

(7) 制定和实施提高全民保护关键基础设施和重要资产意识的计划

国土安全部将与其他重要利益相关人共同评估制定全面提高全民意识计划的需要，用以支持防范工作、安全投资、保护行动的持续发展，同时加强公众对恐怖主义威胁的了解。

提高全民保护意识，意味着全国上下都应认识到，必须将安全从根本上融入到我们的日常

生活和商业活动之中。我们的提高全民保护意识计划应该侧重于关键基础设施工业的具体需要，以支持私营部门根据信息做出的决策，推动相关保护战略和资源配置规划的制定。

这一计划还必须十分全面，足以保持公众对威胁丛生环境的了解，同时增强公众对现行战略和应对威胁手段的信心。

### 技术研发

恐怖主义的威胁要求我们合理配置我们国家的科学技术优势。保护我国关键基础设施和重要资产免受威胁，需要全国做出系统化努力，以充分利用我们的研发能力。唯有如此，我们才能满足保护标准和解决方案提出的诸多紧迫需要，同时还能先进工具和技术的长期发展打下基础，用以在将来制定出更全面、更具成本效益的保护方案，尤其是用以应对我们将来可能遇到的最具灾难性的威胁。

组织全国的工作需要坚持不懈的努力、认真的计划和周密的协调。我们国家的研究事业广泛而复杂。为了研发出能够确保关键基础设施和重要资产安全的先进材料、产品和服务，各种规模的私营公司、大专院校、研究机构和政府实验室都在进行着纯理论和应用方面的研究。

然而，要想把这些优势转化为实际力量，我们必须把确定各部门的需要——标准、工具和流程作为关键性的第一步。这将为研究人员、工程师和基础设施所有者和运营者提供一种指导产品开发的最低能力要求，并为终极用户提供一套衡量他们所用技术有效性的标准。

#### （1）技术研发面临的挑战

利益相关人的数量庞大和成分复杂，说明协调涉及关键基础设施和重要资产保护的技术研发工作会遇到阻碍。各级政府机构以及各关键基础设施部门组织都有各自的研发重点和解决各自最重要问题的利益取向。最初的一大挑战便是在各不相同的需要和努力中找出共同点来，以确定协调哪些方面的研发工作可以给各方带来最大利益。

从整个国家来看，与关键基础设施和重要资产保护相关的长期研究、开发、测试和策划普遍缺乏突出的重点，这是目前我们国内保护工作的严重不足。我们需要一套流程，根据各部门的需要，在全国范围内协调安排科研重点，以支持跨部门的研发工作。

此外，我们的国内保护工作还需要新的工具不断涌现，用以确保运行的安全。在这方面，我们必须不断提高我们检验威胁到我们的食品和农业、供水、大众运输和其他部门的各种污染物（其中包括生物、化学和放射性污染物）的能力。同样，我们还必须不断提高检测和监督能力，以及时发现大规模杀伤性武器及其部件的存在。

我们尤其需要用以支持可以互用的通信的标准。目前这方面的能力缺乏一向是我们国家的保护和应急响应工作的最大不足。现在，联邦、州和地方执法人员以及消防、医疗和应急管理人员使用的是互不兼容的通信系统，这难免给信息交换和安全工作带来困难和障碍。通信设备统一标准的缺乏，无论是在恐怖事件发生过程中还是之后，都有可能严重阻碍安全人员、应急响应人员、州政府应急管理人员和联邦官员之间的密切合作。如果互不兼容的通信连接被恐怖分子利用，我们对恐怖事件的反应可能会变得更加复杂。

对于可以直接进入我们的最关键的设施和系统的人员缺乏鉴别身份的可靠工具，这也会妨碍各部门的安全。在鉴别从事保护和事件处理工作的执法、消防、应急响应人员的身份方面，也存在类似问题。

最后，既要加强安全，同时又要保持商业渠道合理通畅，这种时常会相互冲突的需要要求

我们有新的工具和流程。例如，重要的水坝，特别是那些位于航道上的水坝，面临着严峻的安全挑战。这些水坝的船闸必须保持畅通无阻，但又必须减少来自水上的威胁。其他部门，如航空运输、铁路和海运等，以及重要商业和政府建筑物、国家标志性建筑物等的安全，同样需要有效的防入侵监控和传感能力。

## （2）技术研发工作

为了应对这些挑战，政府和工业界必须共同为物理和信息基础设施制定安全技术标准。这样的标准能够使重要利益相关人更加有效地携手合作，开发对于加强基础设施安全和减轻它们之间互依赖性来说至关重要的产品。

因此，我们将采取以下行动。

### ①协调公共和私营部门的安全研发活动

国土安全部将与其他相关联邦政府机构相互协调，支持安全技术的研发工作，其中包括具体专业的实验计划和项目。这方面的工作涉及建立一种机制，将国防部和其他政府机构开发的技术转让和应用于私营部门基础设施的保护工作。相关行动还包括与我们的国际伙伴适当合作，以扩大我们的研究基础和利用我们的伙伴和同盟者开发的技术解决方案。

### ②协调互用性标准，确保通信系统的兼容性

我们将制定和推广互用性标准，以确保联邦、州和地方政府使用的通信系统相互兼容。联邦通信委员会将与国土安全部、其他联邦领导部门和机构（如商务部国家电信和信息管理局）、其他标准制定机构（如国家标准计量局）、对用户有很大影响的组织以及设备制造商一起领导这一工作。标准的建立将使各级国土安全实体能够使用安全可靠的通信方法。标准化通信系统将增强我们的保护和应急响应能力，同时将提高各个级别的有效规划和培训水平。

### ③开发鉴别和验证人员身份的方法

为了提高我们关键设施、系统和功能的安全系数，我们必须采用更好的手段来识别人员身份。我们必须创建一套统一的方法，用以鉴别执法人员以及进入关键设施和系统的人员的身份。

实现这一人员鉴别计划所需要的技术包括生物计量识别器、磁条和基于微处理器的“智能”卡以及其他系统。这些工具可以使保护和应急响应工作中的人员身份鉴别迅速进行。这种必不可少的加强型“现场控制”可使恐怖事件现场的调查工作顺利进行，同时可为不同分析数据之间的比较设置一条调查基线。

### ④完善监视、监控和检测的技术能力

对于周边、入口和关键节点区域，我们必须从技术上改进我们的监视、检测（包括防入侵检查方法）和监控系统。我们必须开发出更加强大的检测系统，供各关键基础设施部门的安全人员使用。

国土安全部将与其他公共和私营部门利益相关人合作，共同制定研究计划，寻找技术解决方案，弥补关键部门在监视和检测方面的不足，其中包括检测化学、生物和放射性残留物的能力。

## 建模、仿真和分析

建模、仿真和分析活动有助于确定关键基础设施和重要资产保护及相关投资的重点。本战略讨论了基础设施内关键节点和单点故障以及国际国内基础设施部门之间日渐增强的互依赖性提出的挑战和表现出来的不确定性。这些互依赖性和关键节点往往难以识别和解决，它们遭

到破坏会产生跨部门的连锁影响。如果使用得当，建模、仿真和分析可以预测到这些依赖性和互依赖性在各种威胁环境中可能造成的潜在后果。

建模、仿真和分析还可以勾勒出风险环境构成因素之间的复杂关系，从而对保护行动的规划和决策提供支持。例如，仿真特定枢纽的运输流动格局（如模拟某铁路终点站或航空集散站的运输流动格局），便可以分析出攻击该节点有可能在各个方向同时产生什么后果。这样的信息有助于引起对有可能出现的连锁性后果的警惕，而这些可能性否则是不会被考虑到的。

通过建模和仿真，相关部门可以对与特定脆弱性相关的风险做出更精确的评估，从而根据所得信息做出保护决策。建模和仿真还可以用作实时决策支持工具，帮助减轻袭击带来的后果或者完全阻止二次袭击。

私营部门基础设施和资产所有者和运营者在防范和应对洪水、地震和飓风等各种自然灾害方面有着相当丰富的经验。他们深谙应该如何规划和应对，这源自于与这些自然灾害的长期斗争。与自然灾害恰成对照的是，对我们关键基础设施和重要资产的恐怖主义威胁是新近出现的现象。因此，我们缺乏有关这类恶意事件发生模式的类似长期数据，也没有证据显示怎样防御最有成效，这就使建立可靠的替代性数据变得更加重要了。

#### （1）建模、仿真和分析面临的挑战

历史上，我们曾依靠建模、仿真和分析方法对与国防和情报任务相关的决策和规划活动提供支持。现在，我们必须以创造性的方式利用建模、仿真和分析对日趋复杂的决策、风险控制和资源投资提供支持，以应对国内的恐怖主义活动。

建模、仿真和分析对于政府和经济的很多部门都极具价值。这方面的研究可能有很大的需求。就研发规划而言，我们必须在众多项目中找出重点，着重突出那些可以带来普遍利益和体现了最严重威胁和脆弱性的研究项目。

对建模和仿真资源的改善还必须涉及加强数据收集和制定统一标准。当前，很多与国家级保护行动相关的数据要么不存在，要么无法取用，要么不是以标准格式保存的。因此，必须创建和采用数据收集流程、系统和标准，才能将数据以建模和仿真的方式展现出来。

此外，提高我们国家的建模、仿真和分析水平要求公共-私营部门共同做出努力才能取得最佳效果。通过联邦跨部门机构、州和地方政府、国家实验室、学术界和商业企业的有效合作，我们可以为发展这一能力挖掘出大量人才和资源。跨部门的合作对于建立标准方法和统一分析框架、说明研究结果，特别是在对基础设施互依赖性建模时，也是必不可少的。

大多数工业界官员都对企业的运作和相关脆弱性了然于胸。然而，很多企业需要在帮助之下才能识别出它们对其他部门的依赖以及这些互依赖性给他们带来的风险。这种互依赖性的潜在影响在“9·11”事件攻击银行与金融服务部门中表现得淋漓尽致，当时世贸大厦的倒塌阻断了曼哈顿下区的电信服务供应。这次破坏造成电子金融交易中断，由此带来的长期经济影响在一年以后依然阴魂不散。

在多数情况下，建模和仿真能力并没有很好地融合到现行的基础设施保护规划行动中。而这种融合却会把建模和仿真研究数据转化为对具体部门保护规划、决策支持和资源配置的有效指导，这才是至为关键的。

#### （2）建模、仿真和分析方案

我们提出的适合于各关键基础设施部门的建模、仿真和分析方案涉及以下工作。



## ①把建模、仿真和分析融合到国家基础设施和资产保护规划和决策支持工作中

国土安全部将建立一个由公共和私营部门、国家实验室、学术界和商业研究机构代表组成的咨询组，专门研究如何将建模和仿真活动融合到国内保护规划之中。

咨询组将负责对建模、仿真和分析进行研究，然后向国土安全部建议应该把正在进行或规划中的研究活动集中在哪些国家重点项目上。在这一过程的初期，将着重开发和推广模拟部门互依赖性的标准和方法。这类标准所基于的是对被确定是关键性的资产和服务的明确定义，它们将应用到由国土安全部监管的全国协调一致的规划活动中。

## ②开发恐怖袭击短期和长期影响的经济模型

恐怖袭击的经济意义并非总是显而易见的，其短期影响往往只是长期影响的部分先兆。对基础设施遭受物理袭击造成的跨部门暂时经济损失建立模型，有助于政策制定者和应急管理控制专家了解和减轻最坏情况的影响。

## ③提高对关键节点 / 堵塞点和互依赖性进行分析的能力

作为对互依赖性建模和勾勒特定恐怖事件后果的核心目标的基础，我们还将开发度量尺度，用以根据威胁及其影响的等级评估基础设施子系统和关键节点是否设置充分。其中涉及对不同基础设施的坚固性进行比较，因为在这些地方，关键性枢纽中心和关键节点彼此紧密相连，其中一个受到攻击，都会产生连锁性影响。明确国际国内关键基础设施的互依赖性，是我们保护重点项目的重中之重。

## ④就部门预警与预警流程及行动之间的矛盾建模

对预警反应以及和预警系统设计所可能造成的负面影响进行建模，将提高工作的灵活性并减少备份。提高国土安全预警水平的目的是立即对基础设施采取保护措施，挫败恐怖分子的阴谋。但是，这些措施也有可能造成破坏性后果，其交互作用的方式带来了另外的脆弱性。

## ⑤针对网络和物理威胁、脆弱性及后果进行集成风险建模

风险评估有助于识别和确定风险管理和资源配置的方式。这些评估所涉及的威胁分析可以为风险管理和投资决策提供一个基线和参照框架。威胁分析与旨在确定安全系统有效性进而进行后果分析的脆弱性评估结合到一起，将能提供有关关键资产和节点的信息。这类研究中包含了涉及各类网络和物理袭击事件的模型。分析工作将侧重于物理和网络系统之间错综复杂的交互关系，旨在全面确定各种潜在后果，确保研究成果应用到国际国内基础设施保护工作之中。

## ⑥开发改进信息一体化的模型

各部门间威胁和脆弱性信息的一体化必须通过建模实现，这与联邦政府和关键基础设施之间的信息共享要求是一样的，目的是便于找出低效点和丢失的信息。

## 6. 确保关键基础设施的安全

我们的社会和现代化生活方式依赖于复杂的关键基础设施系统。《国土安全国家战略》明确指出了 13 个关键部门。随着我们逐渐深入了解恐怖分子的威胁、攻击手段及其选择攻击目标的标准，这个关键部门列表还会越来越长。关键基础设施部门包括农业和食品、供水、医疗卫生、应急服务、政府<sup>①</sup>、国防工业基地、信息和电信<sup>①</sup>、能源、运输、银行与金融，化学工业

① 本战略的重点是关键基础设施和重要资产的物理保护。每个联邦领导部门和机构都制定了具有连贯性的运作计划，以确保政府对相关工业部门管理的连贯性。有鉴于这些计划的分类，本文将不对政府管理的连贯性进行讨论。

和危险原料、邮政和递送<sup>②</sup>。前文在第 5 章“跨部门安全优先级”中曾经讨论过这些基础设施所共同面临的问题。

本章将对每个部门就以下方面做进一步讨论：

- 该基础设施部门本身以及对其构成支持的工业的独有特点。
- 目前对该部门具体产品和服务供应以及相关关键资产、系统和功能实施的保护。
- 该部门保护工作所面临的独有挑战。
- 该部门需要以合作方式保护的重点。

与本战略的原则一脉相承，任何动用联邦资源的方案都应被各部门视为重点，都应考虑到潜在攻击的风险和后果以及各利益相关人需要共同承担的保护责任。

### 农业和食品

我国的农业和食品工业在世界上是效率最高和生产力最强的。这些工业是美国基本商品的来源地，产值约占国内生产总值的五分之一。它们在美国的出口中也占有巨大比例，来自各种规模农场的产品约占美国出口的四分之一。

农业和食品部门包括：

- 饲料、牲畜和牲畜产品供应链；
- 农作物产品以及种子、化肥和其他相关必需原料供应链；
- 收割后的农产品及其供应链，包括加工、生产、包装、储藏、分销和零售，以及机构食品服务、饭店和家庭消费。

食品生产、分销和消费方式的变化对确保它们的安全提出了新挑战。越来越多的农产品来自国外，很多食品需要经过长途运输，我们越来越频繁地到外面吃饭。公众对农产品以及食品加工和包装系统的信心是维持这些部门经济生存能力的重要因素。同样，美国作为一个可靠的优质、安全食品生产国的声誉是维持外国消费者信心的重要因素。

美国有着强大、运转良好的食品安全系统，可以确保公众不受非蓄意食品污染的危害。除了农产品和食品部门本身采取的安全措施以外，我国的总体食品安全系统还涉及对食品供应链中关键控制点的全面分析，以及联邦、州和地方各级政府对食品加工、储存和包装的严格检查。业内企业正在对他们的设施进行物理安全措施和流程进行评估，其中尤以食品加工厂为重。

#### (1) 农业和食品部门面临的挑战

公众对食品的基本需要以及对食品安全的高度敏感，使确保食品生产和加工的安全成为一大重点。

我国的食品和农业在过去几十年中高速发展，在行业结构上独具特点。食品和农业系统的最大威胁来自疾病和污染。而这些部门的分散化生产对保护工作提出了独特的挑战。过去，政府曾与业界就个别案例的预防蓄意食品污染进行过密切合作。食品安全系统在预防、检测和减轻非蓄意和个别食品污染方面的有效工作为防范蓄意破坏食品供应的行为打下了良好基础。

由于食品系统进入点众多，因此，检测是确保农业和食品部门安全的重要工具。改善和确

---

① 针对具体部门信息技术和网络资产的保护战略在《保护网络空间的国家战略》中有过详细讨论。因此，本文将不对有关信息和电信部门的信息技术保护进行讨论。

② 国家纪念碑和标志性建筑物的保护将在本文第 7 章“保护国家重要资产”中讨论。

立检测食品中生物武器细菌的分析方法，以及扩大实验室规模和提高科研水平是我们当前最迫切的任务。现有的联邦、州和地方公共卫生和农产品实验室是为检测偶尔污染食品的传统人类病菌而设计的。这个系统虽然在预防这些传统人类病菌中发挥着重要作用，但是我们还必须增强这些实验室的能力以便检测出更多种类的非传统病菌。这个得到强化的系统还必须能够消除食品和农产品检测中出现假阳性反应的错误，并能够解决检测的矛盾。

同时，我们还必须扩大实验室系统的规模，以适应预防生物武器对食品供应袭击的需要。我们必须增加能够诊断和治疗牲畜疾病和农作物污染的合格人员（兽医和实验室技术员）和检验员。此外，很多州在食品检查、检测和培训方面的预算需要根据这类方案进行修改。

迁移和加工农作物和牲畜需要长途运输。在运输过程中，这些农作物和牲畜会长时间滞留在库区和类似设施里，从而有可能与其他产品接触。所以，农业和食品部门需要依赖运输系统的所有者和运营者（尤其是卡车和集装箱）来保护食品在运输过程中的卫生和安全。我们必须改进跟踪牲畜和农产品在运输过程中移动的机制，从而使卫生官员可以追查到污染源。

快速获取和使用有关恐怖威胁的信息可以防止单个工厂或某一区域受到的袭击扩散到地区或全国。不幸的是，严重的系统障碍阻碍了这些信息在业内和结构内的共享。比如，很多业主不愿报告食品加工过程中可能出现的问题和污染，因为他们可能会因此而损失收入。

同时，农产品和食品业竞争激烈。很多食品系统中的公司都只有很低的毛利率。因此，一些公司往往会扣留可能的污染事故信息，以防止可能的财务损失。

保护公众不受污染事件损害要求及时报告污染事件，以便能够迅速做出决策和采取行动。在现在的环境下，当被污染的农作物和牲畜需要被销毁或是屠宰时，业内人士对公众负面反应和经济损失的恐惧可能会阻碍农产品和食品部门的反应行动。

恐怖分子的蓄意污染破坏意在使人群和牲畜受到最大伤害。他们的另一个目的是引起公众恐慌和造成经济损失。由于媒体对公众有着巨大影响，与媒体清楚准确地交流信息至关重要。州、地区和国家各级部门都应事先指定官方发言人。虽然食品监管者会定期与业界就食品安全问题进行交流，但是就蓄意污染事件制定双方交流计划也是一大重点，计划中还应明确各利益相关人的责任。

## （2）农业和食品部门保护方案

从部门食品安全流程和规程的评估中获取的信息可以为农业和食品部门关键基础设施保护系统的建立奠定基础。例如，应付牲畜传染病意外爆发的两个重要流程已经建成<sup>①</sup>。虽然这些研究计划是预防动物传染病意外爆发的，但是研究结果和建议也适用于人为蓄意造成的动物传染病。这方面的另一个例子是 1999 年完成的动植物卫生检查报告《保护美国的植物资源》，其中提出的建议目前仍在实施之中。我们需要更深入的研究和合作政策来确定如何改善食品安全系统以应对食品安全问题。

其他农业和食品部门保护方案还涉及如下工作。

### ① 总体评估部门安全现状，确定并解决部门的脆弱性

国土安全部、农业部及健康和公众服务部将与州和地方政府以及业界共同对农业和食品部门进行总体风险评估，确定并解决现存的部门脆弱性。

<sup>①</sup> 这方面的工作详见州农业部研究基金会全国协会 2001 年 10 月的报告《牲畜健康保障综述：结果和建议》以及《美国牲畜健康应急管理系统 2001 年年度报告》。

### ②提高农业和食品系统的检验和化验能力

国土安全部、农业部及健康和公众服务部将与州和地方政府以及业界共同提高本部门检验和化验病菌的能力。建立提高检验能力的各种机制，其中包括技术研发，增加州级兽医、传染病专家和技术专家的人数，这样可以更快地检测出病菌并及时做出反应。增强追查污染源的能力并增加边境和港口的工作人员，也会大幅度增加保护力度。扩大全国各地实验室的规模也会提高分析和反应的速度。

### ③评估与运输相关的安全风险

国土安全部、农业部、健康和公众服务部以及交通部将与农业和食品业界的代表共同评估食品和商品在运输过程中的安全风险，并制定出适宜的解决方案。这方面的问题牵涉范围很广，因此需要将运输安全措施与食品工业已经实行和新近采取的安全措施结合起来进行全面的风险评估。此外，还需统一农业和食品部门报告卡车遭劫和货物失窃事件的方法，并将这些报告在食品工业内通报。

### ④确定潜在的基础设施保护方案；确定和排除障碍

国土安全部、农业部及健康和公众服务部将制定措施和排除障碍，鼓励业内公司及时报告所发生的问题。

### ⑤制定应急响应战略

国土安全部、农业部及健康和公众服务部将与业内相关人员合作，制定一项战略，协调风险信息交流和其他应急响应行动。

## 供水

我国的供水部门在公众卫生和经济中发挥着至关重要的作用。供水部门由两个基本但却是至为关键的部分组成：淡水供应和废水回收及治理。本部门的基础设施多样、复杂且分布极广，其中从只供几个消费者饮用的系统到数百万人服务的设施，应有尽有。在供应方面，关键基础设施保护的焦点是我国的 17 万个公共供水系统。这些供水系统依赖水库、水坝、水井和净水设施以及处理设施、抽水站和管道系统。废水部门的保护重点是 1.95 万个市政下水道系统，其中包括估计为 80 万英里的下水管道。废水处理设施收集和处理家庭、商业和工业污水。废水处理部门还收集和排泄雨水。

供水部门已经采取了很多措施来保护它的关键设施和系统。例如，政府和业界为饮用水和污水设施制定了脆弱性评估方法，并训练了数千名人员专门负责评估工作。环境保护局根据 2002 年《公共卫生安全和生物恐怖主义防范和反应法》开发了可以与脆弱性评估共同使用的基本威胁信息。此外，环境保护局还协助进行了饮用水系统脆弱性评估，并且制定了应急响应计划。

为了改善信息在业内企业之间的流动，供水业开始着手建立本部门的信息共享和分析中心。供水部门信息共享和分析中心将为收集、分析和共享与安全相关的信息提供一个论坛。此外，几个联邦部门共同改进了与污染威胁（如生物、化学和放射性物质被施放进水源等）相关的信息库，同时制定了饮用水被污染时的应对手段。在确定新技术方面，环境保护局有一套现行方案，可用来制定检验协议和验证创新性技术的功能。环境保护局还实施了一项新方案，用于验证可用来检验或避免生物或化学威胁的监测技术。

### （1）供水部门面临的挑战

人类对水的基本需要和维持安全水供应的要求是推动供水基础设施保护工作的主要因素。

公众对国家供水安全的关注，以及在供水基础设施内和附近生活或工作的人员的安全也是很重要的因素。为了确定保护的重点，供水部门正侧重于受恐怖袭击以后会造成重大人口伤亡、财产损失或是广泛经济后果的基础设施。总体来说，供水部门的保护工作共有四个关注重点：

- 对关键资产的物理破坏和摧毁，包括蓄意释放有毒化学药品；
- 实际或威胁污染水源；
- 对信息管理系统和其他电子系统的网络攻击；
- 由其他基础设施引起的服务中断。

为了应对这些潜在威胁，供水部门需要有更多的威胁相关信息才能确定加强相应保护措施的投资方向。供水部门还需要加强监视和分析的能力，以便及早发现水源中被恐怖分子投放的生物、化学和放射性污染物。一些公司已在着手开发更先进的监视和取样技术，但是供水部门需要投入更多的资源。供水部门必须改进环境监测技术和相应的实验室检测能力，以便及时对水源进行分析，确保对水污染的早期预警能力和清理污染能力。供水部门还需在大面积水样分析方法、监测策略、取样方法以及人员培训等方面实现技术突破。

州和地方政府在供水设施出现紧急情况后的应付和处理方法上有着不同的政策和处理步骤。但是，地方和州政府以及联邦各部门必须协调行动，妥善处理水源污染造成的公众反应和公众恐慌。在这个方面，向公众提供及时、必要的信息是保持公众信心的关键。

供水部门的运行在很大程度上依赖于其他部门，其中尤以对能源部门的依赖为甚。例如，输送自来水和回收污水，以及自来水工厂和废水处理工厂的运行需要大量电力。供水部门需要运输系统向其提供大量必需的水处理化学药品，还需要天然气管道系统向其输送必需的能源。自来水和废水处理系统的自动化程度越来越高，远距离高效遥控工厂运转已经成为可能。

#### （2）供水部门保护方案

供水基础设施保护方案是在供水部门面临挑战的情况下以及应最新立法<sup>①</sup>的要求制定出来的。新增保护方案涉及以下几个方面的工作。

##### ①确定需要重点保护的脆弱性和改善设施安全状况

环境保护局将与国土安全部、州和地方政府以及供水部门其他领导机构共同确定进一步确保水坝、抽水站、化学药品仓库、水处理厂等储藏和供应等关键节点安全的必要流程和技术。环境保护局和国土安全部还将向供水部门继续提供必要的工具、培训、技术支持和有限的财政帮助，以利于开展脆弱性评估方法和风险管理战略的研究。

##### ②提高部门的监测和分析能力

环境保护局将继续与业界代表以及其他联邦机构共同改进有关污染的信息系统，同时开发适宜的监测和分析技术和能力。

##### ③改善部门内信息交流和协调应急规划

国土安全部和环境保护局将继续与部门协调员和供水部门信息共享和分析中心共同协调有关威胁、突发事件以及其他与供水部门特殊利益密切相关的信息的交流。国土安全部和环境保护局还将与供水部门以及州政府共同制定标准、协调应急响应和通信协议。

##### ④与其他部门共同管理产生于互依赖性的独特风险

<sup>①</sup> 2002年6月12日，布什总统签署的《2002年公共卫生安全和生物恐怖主义防范和反应法》（简称《生物恐怖主义法》）正式生效。该法要求各饮用水系统进行脆弱性评估，经确认后将评估报告提交环境保护局，同时制定或修改应急响应计划。

鉴于供水部门对其他部门的依赖，国土安全部和环境保护局将组建跨行业工作小组，开发综合各部门保护重点和应急响应计划的模型。

## 医疗卫生

医疗卫生部门牵涉范围极广，业内机构多种多样，包括州和地方政府的卫生部门、医院、医疗诊所、心理健康诊所、养老院、血液供应设施、实验室、火葬场和药品仓库等。

医院、诊所和公共卫生系统在减轻自然灾害和恐怖袭击的后果中发挥着重大作用。这些设施的损坏和服务中断会大大影响整个突发事件处理系统的有效性。即使医院和公共卫生设施不是恐怖分子的袭击目标，它们也可能在化学、生物和放射性物品的攻击下受到污染。

另外，全国医疗网的建立依赖于我国的几个主要专业化实验室设施和资产，尤其是那些与疾病控制和预防有关的设施，如健康和公众服务部所属疾病控制和预防中心、国家卫生研究所和国家战略物资仓库。

### (1) 医疗卫生部门面临的挑战

医疗卫生工作人员已经习惯于在威胁下开展工作。但是，他们通常不认为自己是恐怖分子的袭击目标。

大部分医院和诊所都可以自由进入，因为它们在向公众提供很多必不可少的服务。但是，这种自由进入也大大复杂化了我们发现潜在恐怖袭击和预防恐怖分子进入的工作。另外，我们还缺少确定潜在传染病患者的方法和标准。这两个方面的事实对设施的安全保卫和应急响应处理有着很大影响。

另外一大挑战是医院和诊所的结构和系统设计五花八门、复杂多样。一方面，所谓“免疫建筑”有着阻隔传染病传播的设计结构，包括空气流通控制、隔离病房和可以消除传染病病菌传播的特殊建筑表面；另一方面，很多建筑几乎没有环保的内部设计结构。对这种建筑物的保护对我们提出了极大的挑战。

在传染病流行时期，已被传染的病人在社区内的自由活动会构成极大的公共卫生风险。医疗卫生部门必须制定出控制和隔离传染病人的综合计划和方案。

医疗卫生部门面临的其他挑战与存储、保护和配送关键应急药品有关。现在，除了国家战略物资仓库之外，我们没有足够数量的设施来补充和储存关键物资和关键药品。我们还需要改善医药用品供应链管理，以确保医疗卫生业在紧急状况下的安全和有效运转。复杂的法律和税收规定对可能的解决方案有着极大影响。当前，联邦政府对相关公司的医药用品库存只有有限的管理权限。由于医药公司需要为其产品库存纳税，它们往往避免大量库存积压，只是通过及时的生产来满足需求。

针对本部门的法律法规问题也会阻碍保护这些资产和服务的效果。《紧急医疗处理和主动劳动法》规定医院必须治疗急诊病人，而不能顾及病人是否上有医疗保险。有着大量伤亡的灾害情况会大大消耗这些关键基础设施的人力、药品供应和病房资源。当病人的病情稳定之后，我们通常需要将他们转移到其他医院，以便为新到达的病人腾出病床。但是，对于那些没有上保险的灾害病人来说，一旦病情稳定之后，医院将不再有给他们实施治疗的义务。因此，很多二级的非关键医院不会接收没有上医疗保险的病人。这就需要关键医院继续对他们进行治疗。另外，《健康保险可携带性和责任法》中的保护隐私条款可能需要修改，因为这些规定可能在传染病散播期间妨碍关键信息的共享。

现有的安全挑战决定了医疗卫生部门的工作重点是评估危机时期提供必要服务的能力。但是，很多医院利润很低，从而不能在安全设施方面作大量投资。

最后，我们应该特别关注专业医学和药物实验室，尤其是那些处理剧毒和传染病菌的实验室。这些设施在确定哪些病菌在袭击和疫情爆发中最危险方面发挥着重要作用。它们还可以控制、消除和处理有毒物质。增强对这些专业机构的安全保卫是我们最重要的任务。

## **（2）医疗卫生部门保护方案**

医疗卫生部门的保护方案涉及以下几个方面的工作。

### **①任命值得信赖的发言人**

健康和公众服务部将与州以及地方政府卫生官员共同确定、任命和培训得到认可的特定事务专家以在危机发生时充当医疗卫生部门发言人。这些专家将作为国土安全信息的特使对外公布内容一致的准确信息，并告诫美国公众必须采取什么行动。此外，健康和公众服务部还要准备发挥重要作用，在全国范围内对公众发布有关生物恐怖袭击或威胁公共卫生的其他突发事件的信息。

②审查关键任务的执行情况、确定保护重点、确保关键实验室设施和服务安全、允许适度配备备用设施

健康和公众服务部将与医疗卫生部门的医院和诊所共同审查它们的关键任务系统及其执行情况，帮助它们制定确保重点安全投资和提高保护水平的详细计划。健康和公众服务部及国土安全部还将与各州卫生部门合作，共同确定重点国家级医院和医疗中心以及它们最重要的组成设施、系统和服务。

健康和公众服务部及国土安全部将与医疗卫生部门共同确保重要实验室设施的安全，同时允许适度配备备用关键能力和数据系统。

### **③提高监视和交流能力**

健康和公众服务部将协助医疗卫生部门人员确定建立严格监视系统的需求，同时协调医疗卫生监视设施与医疗服务系统之间的联系。

### **④制定隔离传染病标准**

健康和公众服务部将与州和地方政府卫生官员共同制定隔离检疫标准和制度，以便在卫生危机时期进一步保护那些未被传染的人群。健康和公众服务部将与州和地方政府卫生官员在制定后果管理规划的过程中共同确定在恐怖分子进行生化袭击时应该重点使用哪些疫苗和预防资源。

### **⑤开发增加安全设施投资的选择方案**

健康和公众服务部将与各州卫生部门合作，共同研究和修改有可能阻碍关键卫生设施在危机时期提供关键服务的法律规定。另外，健康和公众服务部还将开发可能的方案，以鼓励增加对医疗卫生部门基础设施物理保护的投资。旨在提高地方社区关键医院能力的现行联邦拨款投资计划是这方面工作的一个良好起始点。

## **应急服务**

应急服务基础设施包括消防、营救、紧急医疗服务（EMS）和在突发事件、自然灾害或恐怖袭击中拯救生命和财产的执法机构。

### （1）应急服务部门面临的挑战

“9·11”恐怖袭击事件的教训说明，本部门必须解决的最迫切问题是：各机构之间的信息共享极不充分，其中尤以执法部门与其他第一反应部门之间的信息共享为甚；通信问题，例如缺乏足够的备用设备；加强犯罪现场控制和提高安全保卫防止第二次攻击等多个方面。

恐怖分子对我们国家的应急响应网络提出了严峻挑战。虽然现有基础设施足以应付常规突发事件和地区性灾难，但是“9·11”事件说明我们缺乏足够的应付大规模恐怖袭击以及其他大规模灾难。这样的灾难需要联邦、州和地方各级应急服务部门密切合作。在所有问题之中最亟待解决的是，即便在同一地区的各第一反应部门，如警察和消防部门之间也不能进行协调合作。

重大紧急事件需要多个部门和当地社区的密切合作。但是，各部门的人员和应急响应系统都是根据各部门的不同特点和需要设计的，从而造成各个部门之间无法顺利合作，极大地阻碍了各第一反应部门在危机时刻的救援能力。

良好的通信系统是在危机和紧急情况下确保人员安全和有效部署人力资源的保证。通信系统失去运转能力将会大大降低各部门的反应速度，并会给救援人员带来生命危险。另外一个重要问题是紧急情况下的通信在很大程度上依赖于几个关键的物理节点，如总调度台、消防队和911报案中心。

跟大多数与物理系统紧密相连的关键基础设施不同，应急服务部门由高度机动的专业人员小组和设备组成。因此，应急服务部门面临的另一严峻挑战是，必须在突发事件反应行动中确保第一反应人员和关键设备的安全。未来的恐怖袭击可能会在袭击现场出现不明的危险，其中涉及生物、化学和放射性物质。此外，以往的经验表明，应急服务部门的人员和设施也可能成为直接袭击或二次袭击的目标，而通畅通信的缺乏以及应急响应部门的准备不足，会使原本就十分糟糕的情况更加恶化。

预防性演习可以为反应和紧急情况管理准备工作提供经验和反馈信息。州、地方和联邦政府举行过地方或地区性演习。各地采用的方法有很大差异，这也阻碍了多部门协同反应的效果。

面对重大恐怖袭击的威胁，任何地区都没有能力维持和调动全部资源进行有效反应。互助协议可以打破司法界线，大大便利安全人员、设备和其他主要资源的跨区域流动，从而使地方社区得以互相帮助应对紧急情况和灾难性事件。

### （2）应急服务部门保护方案

应急服务部门的保护和反应方案涉及以下方面。

#### ①采用通用通信系统

国土安全部和司法部将与州、地方政府以及其他相关单位共同研究和解决重要通信系统的通用问题。这个问题已在州和地方政府一级得到广泛认识。确保紧急情况下通信畅通无阻的高于一切的共同需要是推动各部门共同寻求解决方案的催化剂。

#### ②开发备用通信网络

国土安全部将与州和地方政府官员共同开发应急响应备用网络，以供出现大面积通信中断时使用。

#### ③采取措施保护国家应急响应基础设施

国土安全部将确定和分析我国应急响应基础设施（其中包括关键人员、设施、系统和功能）的脆弱性。国土安全部将与州、地方政府以及其他实体共同制定计划，在确保应急响应关键基



基础设施安全的同时，确保应急响应中人员的安全。

#### ④协调全国性预防演习

国土安全部将与州和地方政府共同制定一项协调一致的全国应急响应演习计划。协调一致的预防演习可以在地区和全国层面上推动保护规划、反应协议和反应能力的步调一致，同时可以为交流经验和最佳实践措施提供一个论坛。

#### ⑤推动和强化地方政府之间的相互援助协议

国土安全部将与地方社区官员共同强化现有的相互援助协议，同时在必要的情况下制定新的地区间相互援助协议。此外，国土安全部还将就采用何种通用标准以及设备和培训术语发起展开讨论。

### 国防工业基地

我们国家的国防和军事力量主要依赖国防部和私营国防工业的支持。没有私营部门的重大贡献，国防部不可能有效执行国防任务，如军事动员和在海外部署军事力量等。反过来，私营工业和公众也在很大程度上依赖联邦政府对国家的防卫以及对我们在国内和国外的利益的保护。

反恐战争的成功取决于美国军事力量的快速部署以及进攻和防卫的能力。而军队的训练和装备是确保这个能力的重要因素。私营工业为武装力量提供了大部分装备、物资、服务和武器。几十年来，国防部已经确定了自身的关键资产和系统。同时，国防部还在开始解决它对国防工业基地的依赖问题，如今正在充分考虑私营部门对保护关键基础设施的意见。

市场竞争、企业兼并和全球化减少或消除了备份的生产和服务能力，从而大大增加了国防部面临的风险。外部采购和复杂的国内国际企业兼并使国防部越来越难以确保其主承包商的第二至四级承包商对安全保卫要求的认识，从而无法指望它们在国家出现紧急事件时提供支持。

#### （1）国防工业基地面临的挑战

过去 20 年，国防部对私营工业的依赖越来越严重。国防部已把越来越多的从前由军方独立完成和控制的任務交给承包商来做。甚至于很多为重要军事机构服务的公共事业公司也都已经私营化了。由于市场竞争和摩擦，国防部越来越依赖单个或少数几个私人承包商来满足其大部分需求。与其他联邦部门不同，国防部要求有严格的产品规格和独特的服务要求，因此，某个私人承包商可能是世界上唯一可以满足这些要求的供应商。

另外一个相关问题涉及国防部与私人承包商签订提供关键服务和设备合同的现行流程。大部分合同签署流程所依据的是成本效益。这种方式可能并不总是考虑了供应商保护基础设施的因素（如工人的雇用和原材料的供应），以及它们在紧急情况下提供大量产品的能力。

最后，私营部门也越来越担心联邦政府加强保护基础设施的规定会提高它们的成本和带来更多的风险。

#### （2）国防工业基地保护方案

私营国防工业的基础设施已在很大程度上与国防部的基础设施紧密结合在一起了。国防部和国土安全部将继续与私营部门合作，共同确定关键基础设施并对其实施保护。此外，国防部和国土安全部还将与重要国防工业基地企业合作，将各企业的现有保护计划结合起来，融合为一个整体。

新增国防工业基地保护方案涉及以下几个方面的工作。

##### ①将关键基础设施保护要求融入合同流程和规程之中

国防部将与国防工业密切合作，重新审定合同签订的流程和规程，以确定如何将满足关键基础设施保护需要的条款写入合同之中。合同将具体规定国家紧急情况的要求，如承包商的反应时间、原材料和劳动力的使用、直接的后勤支持等。如果合适，合同还将规定项目经理保护支持性基础设施的责任。敏感的合同文件在对外公布之前将得到更严格的审查和修订。此外，国防部还要重点检查其对外国公司和供应商的依赖程度。

②探索生产和配送流程和规程中的安全问题

国防部将与业界共同研究如何消除生产和配送各个环节中的瓶颈制约因素。

③开发国防部门与私营服务供应商之间有效安全信息共享的方式

国防部将与国土安全部以及情报和执法部门共同制定和建立必要的政策和机制，以推动与国防工业的安全信息交流。

## 电信

随着技术高速发展、商业竞争愈演愈烈以及监管环境不断变化，电信部门也在不断发展着。但是电信部门的动态特征并不妨碍它提供可靠的、满足政府和商业需要的通信服务。在新的恐怖威胁的环境下，电信部门面临着如何保护其数量庞大、布局分散的关键资产的严峻挑战。由于政府和很多关键基础设施部门在很大程度上依赖公用通信设施，对电信部门关键设施的保护显得尤为重要。

电信部门通过一系列复杂的公共长途通信转换网、互联网和私营网络为政府和私人用户提供数据和语言传输服务。公共长途通信转换网为电话、数据和点对点服务提供交换电路。它包含的物理设施有 2 万多个交换机和其他设备。这些设备通过 20 亿英里的光纤和铜线连接。公共长途通信转换网的物理设备是电信部门的中枢，而蜂窝、微波和卫星技术则为更多的用户提供了无线网络。为公共长途通信转换网提供支持的有营运商、管理者、维修人员和供应系统。供应系统提供了很多重要的管理功能，如结账服务、会计服务、安全管理服务等。

数据网络技术的进步和日益增长的数据需求推动了互联网设施的高速发展。互联网由使用一组共同网络协议的全球包交换网络组成。互联网服务供应商向最终用户提供互联网接入服务。大规模互联网服务供应商使用网络运营中心来管理它们的大容量网络。小规模互联网服务供应商通常向大规模互联网服务供应商租用设备和通信容量，并向本地最终用户提供网络服务。互联网服务商通常通过网络中心的交换机和路由器与公共长途通信转换网互相连接。国际公共长途通信转换网和国际互联网之间的信号传送是由海底电缆连接的。

除了公共长途通信转换网和互联网之外，企业网络也是电信基础设施的一个重要组成部分。企业网络是为大型企业的语音和数据传输服务的。这些网络包括向公共长途通信转换网或互联网服务供应商租用的网络线路。

1996 年《电信法》将竞争机制引入了地方公共长途通信转换网。该法规定现有运营商必须允许竞争者使用其网络。因此，电信营运商开始将它们资产集中到被称为“电信饭店”的中心设施之中，而不是铺设新的电缆。互联网服务供应商同时也开始集中到同一设施之中，以便降低与其他服务供应商交换数据的成本。因此，开放的竞争已使公共长途通信转换网和互联网（包括交换机、传送、信号、路由器、控制、安全和管理）更加紧密地连接起来，并且使用同种的软件，进行远程管理，而电信部门的物理资产越来越集中于公用的设施之中。

电信基础设施正经历着从传统的电路-交换机网络到宽带信息包网络（包括互联网）的重

大转变。最终，信息包网络会代替传统的电路-交换器网络，并且建立以公共的、宽带的、多元化的、大规模的以信息包为基础的下一代网络。另外，电信基础设施的发展变化包括了移动电话服务和应用的持续增长。无线通信营运商通过其基地的基础设施和遍布其服务区域的发射塔来传递信息。无线服务包括数字化移动电话和新兴起的数据服务，包括互联网通信、无线局域网和更先进的电话服务。

下一代网络的发展和新的无线服务的出现在继续增加电信部门的物理基础设施。政府和业界需要共同制定确保这些基础设施可靠性和安全的策略。政府和私营部门正在合作解决电信安全的问题，合作的机构包括国家安全电信总统顾问委员会、关键基础设施保护委员会、政府网络安全信息交换中心、电信信息共享和分析中心、网络可靠性和公用性委员会和联邦通信委员会。这些机构提出的解决方案将极大地提高电信部门正在发展中的基础设施的安全性和可靠性。

#### （1）电信部门面临的挑战

电信部门的物理基础设施每天都面临着传统自然的和人为的威胁，如天气变化、无意造成的电缆断线、内部人员威胁（物理破坏和网络破坏）。“9·11”事件揭示了恐怖分子对电信部门基础设施的威胁。虽然电信部门不是袭击的直接目标，但它还是遭受了巨大的间接损失。将来，某些重要电信基础设施集中的地域很可能会成为恐怖分子的直接攻击目标，尤其是那些使用率越来越高的配置设施。电信基础设施经受住了“9·11”恐怖袭击事件，表现出很强的安全性和韧性，因为多样性的备用通信设备很快就替代了被破坏的通信设备。

电信营运商需要优先解决的问题是服务的可靠性、成本平衡、安全性和风险管理的有效性。政府则要优先考虑建立保护基础设施的统一的安全措施。尽管私营-公共部门的利益相关人有着相似的目标，但是他们对于可接受的风险和如何确保基础设施的安全和可靠性的看法却各不相同。因此，双方在可持续的最低安全标准和相应的安全要求方面达成一致意见尚有待时日。

由于各关键基础设施之间互依赖性越来越强，因此对其中一个基础设施的直接或是间接攻击会对其他基础设施产生连锁影响。这种互依赖性增加了确认关键资产和保护其免受物理和网络攻击的必要性。其他关键基础设施依赖于电信部门基础设施的安全和正常运转。配备备用设备是避免因某一节点损坏而带来巨大损失的重要手段。政府与电信部门共同了解该行业的多元性结构特点并制定出最佳保护策略是解决问题的关键。

尽管面临着如此艰巨的挑战，电信市场依旧竞争激烈，消费需求维持在很高水平。行业生产力的提高会大大增加服务需求。联邦通信委员会和市场力量会共同确保电信部门的持续发展并维持可靠的服务水平。然而，最近的经济衰退已经迫使业内公司将其现有资源使用在基本网络运营上，而不是使用在提高能力、确保安全和强化基础设施上，原因可能在于对后者的投入势必会扩大必要的基础设施保护投资对公司财务的影响。

#### （2）电信部门保护方案

由于电信部门所面临的物理和网络威胁，政府与业界必须继续合作，共同了解本部门的脆弱性、采取相应措施、制定政策和规程、提高降低风险意识。电信部门有着与政府合作解决电信基础设施可靠性和安全问题的悠久历史。该部门最近实施了一系列新方案以进一步确保可靠性以及快速恢复和重建能力。在这个越来越重视保护问题的环境下，公共-私营部门需要通过更深入的合作来实施各种重要的电信部门保护方案，其中涉及以下若干方面。

##### ①制定适宜的最低安全标准

国土安全部将与业界共同制定适宜的部门最低安全标准，并依据这一标准提出一系列安全

要求。国土安全部将与业界共同努力，缩小双方在安全预期和安全要求方面的差距。就确保物理多样性的方法达成一致意见是这方面工作的重点。

#### ②提高基础设施多样化数据发送能力

国土安全部将推动提高政府定义和勾勒电信部门全景结构的能力。这方面的工作涉及确定各基础设施之间关键连接点和引导制定能够更好地解决安全和可靠性问题的战略。

#### ③了解与电信基础设施脆弱性相关的风险

电信部门的基础设施（包括公共长途通信转换网、互联网、企业网络和私营网络）向各级政府和其他关键基础设施提供了必要的通信服务。国土安全部将与该私营部门共同开展研究，了解电信基础设施内的物理脆弱性及其相关风险。这方面的研究将侧重于那些集中了多种设备和多个通信营运商的设施。

#### ④协调与主要盟国和贸易伙伴的关系

我国电信部门的安全和可靠性也在很大程度上依赖我们的盟国和贸易伙伴的通信设施。国土安全部将与其他国家合作，共同寻找可以优先与我国政府、全球性工业和网络连接的具有创新性的通信方式。唯有如此，才能确保重要的通信联络。

### 能源

能源是当今美国社会很多高尖端流程得以运行的基石。它是维系我们的经济、国防和生活质量的关键要素。

就关键基础设施保护而言，能源部门通常分为两个部分：电力及石油和天然气。电力工业每天为将近 1 300 万个家庭和机构服务。2001 年，美国消耗了大约 3.6 万亿度电。石油和天然气部门的设施和资产<sup>①</sup>分布极广，其中包括 30 多万处生产场所、4 000 个海上石油平台、600 多个天然气加工厂、153 个炼油厂、1 400 多个石油产品输送终点和 7 500 多个加油站。

### 电力

几乎每种生产活动，不论是在公司、工厂、学校、医院还是家中，都离不开电力。电力也是生产其他能源的必需品，如提炼石油。如果大范围发生长时间电网中断事故，很多对于我们的经济和国防来说至关重要的活动，包括事故调查和修复工作都将无法进行。

北美的电力系统互相连接的多点配送系统，负责所有美国、加拿大和部分墨西哥的电力供应。系统包括三个主要部分：发电部分、输电和配送部分以及控制与信息交流部分。

发电部分的资产包括火力发电厂、水电厂和核电站。输电部分系统将全国各个地区相互连接。配送系统将电力输送到家庭和工厂。控制与通信系统操作和监视相关的关键基础设施。

除了这些组成部分外，电力基础设施还包括那些确保燃料供应的附属设施与系统，其中有些设施涉及危险原料的处理。电力部门的发电还高度依赖其他关键基础设施，如电信和运输。

北美电力系统是最可靠的电力系统，这在很大程度上归功于全行业为确定系统脆弱性和系统互依赖性以及适度设置备份流程、系统和设施而付出的努力。

在 1965 年纽约大停电之后，电力业建立了北美电力可靠性委员会，负责制定防止类似事故发生的指导方针和步骤。北美电力可靠性委员会是一个非营利性组织，由 10 个地区性电力

---

① 输送石油和天然气的管道是交通部门关键基础设施的组成部分，其安全由交通部负责。它们的保护将在本章“运输”一节中详细讨论。

可靠性委员会组成，成员包括美国和加拿大公共和私营电力公司。北美电力可靠性委员会大大提高了电力业安全性。

电力业是被严格监管的行业。联邦能源监管委员会和州公用事业监管委员会是行业监管的主要政府部门。原子能监管委员会则是监管核电站反应堆核以及其他民用核设施、核材料和相关活动的部门<sup>①</sup>。

#### （1）电力部门面临的挑战

电力部门十分复杂，其大量组成资产和系统遍布北美大陆各地。该部门的很多重要资产，如发电设施、变电站等为保护工作带来了独特的挑战。

电力部门内愈演愈烈的竞争和不断的结构变化可能会改变电力市场参与者的安全责任。这些利益相关人规模、能力不同，关注重点各异。现在，单个的公司需要独自支付对安全系统的投资。通常，这些公司会寻求提高电价来回收对安全系统的投资。然而在现行联邦法律规定下，电力业参与者并不一定就能被允许通过提高电价来回收联邦规定的安全措施的成本。

电力业面临的另一挑战是行业内部的有效信息交流。电力系统的所有者和运营者包括各种各样的集团。行业协会是业界信息的发布机构，但并非所有业界所有者和运营者都加入了协会。对基础设施互依赖性进行全面分析所需的信息根本就无法得到。

对于某些电力输送和配送设施来说，配置备份设备和增加生产能力可以为供电服务的可靠性提供更大的保障。然而，这种方式也面临着各种挑战。过长的交付周期、通行权的可能被拒绝、州和地方政府的定线要求、把守“自我地盘”的观点以及与竞争性投资需要相比较时的回报率的不确定，都阻碍了电力设施所有者和运营者对安全和服务保障措施的足够投入。

建立一个脆弱性较低的电网是保护国家电力基础设施的另一个选择。为电力部门制定一项全国性研发战略的工作正在进行之中。此外，联邦能源监管委员会也制定了研发指导方针，能源部的全国电网研究报告就如何提高输电系统的物理和网络安全提出了建议。

#### （2）电力部门保护方案

长期以来，电力部门一直在积极采取各种措施确保电力供应的稳定和可靠。各电力企业也与当地社区积极合作，共同解决与电力系统和电力设施相关的公共安全问题。自 2001 年 9 月 11 日以来，电力部门已经重新制定了安全指导方针，并建立了一系列工作小组负责解决电力部门独有的安全问题。电力部门成立了一个由各公司首席执行官组成的行业安全委员会，用以强化规划、提高认识和改善业内资源配置。

从 1998 年起，电力部门作为一个整体，以国家能源监管委员会为部门协调员，一直在与能源部共同评估电力部门在新的威胁丛生环境下所面临的风险，其中尤以电力系统对信息技术和网络的依赖为评估重点。

在管理安全信息方面，电力部门已经制定了一个提示、分析和警报计划，用以就突发事件报告和预警流程对公共事业公司人员进行培训。该部门设置了物理和网络事件威胁警报级别，内容包括每个警报级别的行动反应指南。电力业还建立了信息分析和共享中心，用以收集突发事件信息、中转警报通告和在联邦政府与全国各地电力网运营者之间协调每日汇报。

电力管理控制中心是电力网中最需保护的地方。联邦能源监管委员会的指导方针要求电力

---

<sup>①</sup> 核电站是能源部门的一个重要组成部分。由于对核设施的袭击有可能对公共卫生和公众安全带来危险后果，有关核设施的具体保护问题将在第 7 章“保护国家重要资产”中详细讨论。

企业建立备份系统和人工操作区。联邦能源监管委员会还在与电力部门共同制定一系列电力企业供电安全要求。

新增的电力部门保护方案涉及以下几个方面的工作。

①确定设备备份要求

国土安全部和能源部将与电力部门共同列出对于电力系统正常运转来说至关重要的成分和设备，确定和评估可以加强修复和恢复工作的其他方法，其中包括设备实现标准化和提高成分的可互换性等。

②重新评估全国性保护规划以及应对袭击的系统修复和恢复

电力业有着从破坏性事件中重建和恢复的良好历史和记录。业界需要与政府共同评估这个系统，并将地区性系统融合到全国性综合反应系统之中。国土安全部和能源部将与电力部门共同合作，确保现有的协调和相互援助流程在电力部门的结构体系不断发展的过程中能够有效和高效支持保护、反应和恢复行动。

③制定降低脆弱性的战略

国土安全部和能源部将与州、地方政府以及电力部门共同确定电力系统关键设备的备份水平，以及出于行业重新调整和重建目的的设计和 implement 备份计划的要求。

④为物理安全计划制定标准化指导方针

国土安全部和能源部将与州、地方政府以及电力部门共同制定评估关键性、关键设施脆弱性和风险评估标准方法和电力部门人员物理安全培训的统一标准。

## 石油和天然气

石油和天然气行业是紧密联系在一起的。石油基础设施包括五个主要的组成部分：石油生产、原油运输、提炼、石油运输和配送以及控制和其他外部支持系统。石油和天然气的生产包括勘探、开采、生产、收集系统及其支持设施。原油运输包括石油管道（16 万英里）、存储、港口和运输船只。石油提炼基础设施包括大约 150 个大小不等的炼油厂，每天的石油产量从 5 000 桶到 50 万桶不等。石油的运输和配送系统包括管道、铁路、船只、港口、油库、卡车和加油站。

天然气业包括三个主要组成部分：勘探和生产、运输以及配送。美国天然气产量约占世界总产量的 20%。全国有 27.8 万英里天然气管道和 120 万英里石油配送管道。

石油配送包括油库存储设施、汽油加工、液化天然气设施、管道以及加油站。天然气的存储指那些地下的蓄水层、废弃的石油和天然气钻井以及岩洞等。

石油和天然气工业的管道和配送系统也是被严格监管的。监管涉及财务状况、安全、开采选址等。业界在勘探和生产方面所受的监管不是那么严格。

（1）石油和天然气部门面临的挑战

关键资产的保护要求提高安全意识和增加对保护性设备和系统的投资。一大严重问题在于，在确定和判断公司安全支出方面缺乏度量标准。在遇到自然灾害和事故时，有一套成熟的方法可用来确定对保护性设备、系统和风险管理手段（如投保）进行投资的风险和成本效益水平。然而，究竟什么水平的安全和保护在应对恐怖袭击风险上是适度和高成本效益的，却是含混不清的。

遇到恐怖袭击时，最先赶到石油和天然气设施现场的政府反应人员是地方警察和消防员。

总的来说，政府反应人员需要提高他们处理计划周密、使用尖端技术的袭击，尤其是使用生化和放射性武器的袭击能力。幸运的是，因为公共安全的要求，石油和天然气业的大部分设施都已经采取了行之有效的保护措施。

在紧急情况下迅速修复被破坏基础设施的工作受到诸多因素阻碍，其中包括申请地方、州和联邦建筑许可证或免除许可证的时间过于冗长，提交环境审查和影响陈述报告的要求过于严格以及申请铺设管线连接相邻设施的建筑通行证的手续过于复杂等。是否能够得到必要的材料和设备以及这类设备的独有特性也是迅速重建被破坏基础设施的障碍。

计划和配送备件的现行系统需要得到大幅度强化。其中有些系统是最新和最先进的，但也有些系统是几十年前的陈旧设备。虽然新系统都是标准化的，但是很多老零件却是非标的，必须专门定做。此外，天然气设施在规模、所有权和安全方面差异很大。而且，数量庞大的天然气设施散布全国各地，这也使保护工作大大复杂化。

## （2）石油和天然气部门保护方案

石油和天然气部门的保护方案涉及以下几个方面的工作。

### ①规划对石油和天然气业研发工作的投资以增强行业的活力和可靠性

国土安全部和能源部将动用联邦政府的国家科研力量，与石油和天然气部门利益相关人共同制定一项研发战略，以适应保护、反应和恢复的要求。

### ②制定降低脆弱性的战略

国土安全部和能源部将与州、地方政府以及业界共同确定关键设备和系统的适宜备份水平，同时确定设计和提高可靠性的要求。

### ③为物理安全计划制定标准化指导方针

国土安全部和能源部将与石油和天然气业界代表共同制定评估关键性、关键设施脆弱性和风险评估标准方法和业界人员物理安全培训的统一标准。

### ④为设施和系统的重建措施制定指导方针

国土安全部和能源部将组建一个由来自本部门、建筑公司、设备供应商、石油工程公司以及地方、州和联邦机构的代表组成的顾问小组，负责确定适宜的规划要求和方法。

### ⑤建立一个支持反应和恢复行动的全国性关键配件计划和配送系统

国土安全部和能源部将与业界共同制定地区性和全国性方案，用以确定配件和要求、通报配件齐备并将其配送到应急响应现场。

## 运输

交通部门由航空、海运、铁路、管道、高速公路、卡车运输和客车运输、公共运输等主要运输方式组成。交通部门的多样性和规模使其成为保障我们的经济和国家安全（其中包括国防动员和军事部署）的至关重要因素。总的来说，交通部门的基础设施十分完善，几十年来在政府和私人双重投资下一直稳定发展。各种运输方式为我们的社会提供了移动性，并且使我们国家珍贵的个人自由成为可能。运输基础设施还非常便利。美国人的日常生活依赖于运输设施的方便性和可靠性。

交通部门与经济的其他每个部门之间几乎都存在着互依赖性。因此，对交通部门的威胁会危害到其他依赖交通部门的行业。

## 航空

航空业规模庞大，由数千个接入点组成。它还具有象征意义，代表着在美国人的价值观中具有极高地位的移动自由以及使美国成为世界强国的技术和工业。我国的航空系统包括两个主要组成部分：

- 机场及其附属资产，包括飞机；
- 航空控制中心、通信中心和信息系统中心。

在“9·11”恐怖袭击之前，机场及其附属资产的安全由私营航空公司、州和地方的机场所有者和运营者负责。在“9·11”事件之后的几个月里，国会通过了建立运输安全管理局的法案。运输安全管理局将负责机场及其附属资产的安全。

### （1）航空业面临的挑战

“9·11”事件表明，航空业对于美国经济以及由经济提供给公民的自由的至关重要使对这个行业的保护成为国家的一大重点。航空业面临着若干种独特的保护挑战。它的广泛分布以及可以从国内外数千个接入点进入的开放性，使确保该行业的安全十分困难。此外，航空基础设施的成分不仅是恐怖袭击的明显目标，同时还有可能被恐怖分子用作攻击武器。所有这些因素加在一起，使美国航空基础设施成为未来恐怖袭击的一大潜在目标。

航空业保护工作面临的其他挑战还包括以下方面。

- 运载量：美国飞机每天运载着数百万乘客以及数量至少是乘客两倍的包裹和其他货物。
- 有限的功能和空间：当前用于检测的设备和方法在数量、功能和使用便利方面都十分有限。
- 时间要求高的货物：及时发送贵重货物对于很多企业来说是基本要求。对这类货物处理和运输的任何长时间延迟都会对美国经济产生负面影响。
- 安全与方便的矛盾：在减少堵塞和延迟的同时又要确保安全，这使保护工作变得非常复杂，但是具有重要经济意义。
- 可进入性：大多数机场都是对公众开放的；机场设施靠近高速公路，便于车辆把乘客送入航空集散站。

航空业的另一关注问题是在持续高度戒备时期增加安全措施的额外成本。自 2001 年 9 月 11 日以来，全国各地的机场一直在实施保护措施方面超负荷运转，以求能够满足当前威胁环境的安全要求。有些现金羞涩的运营者不得不通过降低业务量来维持提供更高级别安全措施的平衡。

### （2）航空业保护方案

“9·11”事件中机场安全保卫工作的失败使航空业遭到社会各界的猛烈批评。为了重新获得公众对航空旅行的信任，公共和私营机构加大了对机场安全保卫的投入。很多措施仍在实施之中。作为运输业联邦领导部门的国土安全部将与交通部、业界以及州和地方政府共同组织、规划和开展必要的保护行动。

航空业保护方案涉及以下几个方面的工作。

- 确定脆弱性、互依赖性和补救要求

国土安全部和交通部将与来自州和地方政府以及业界的代表共同实施或推动评估工作的展开，以确定脆弱性、互依赖性以及运行和协调中心设施和系统的补救要求（如为空中运输指



挥控制中心备份通信设备的需要等)。

➤ 确定对乘客的潜在威胁

国土安全部和交通部将与航空公司和机场安全官员共同开发或推广确定可能的人为威胁的新方法，同时尊重宪法规定的自由和隐私权。

➤ 改善关键出入口的安全

国土安全部和交通部将与航空公司和机场安全官员共同加强或提高机场候机区受限出入口以及机场周边地区和相关设施（其中包括运营和协调中心）的安全。

➤ 提高货物检查能力

国土安全部和交通部将与航空公司和机场安全官员共同确定、采用或推广可加强机场货物检查能力的技术和流程。

➤ 确定和改进检查技术

国土安全部和交通部将与航空公司和机场安全官员共同采用或推广强化型爆炸物检查技术。这样的设备可以减轻越来越严格的保安措施给办理登机手续的乘客带来的影响，同时也可以为确保航空安全提供更有效和效率更高的手段。

### 客运和货运铁路

在每天的每个小时，都有火车在美国大地上穿行，把原材料生产者与制造业生产者以及零售商连接到一起。火车运输矿产品、工业品、农产品、液态化学物品、燃料和消费品。铁路负责了 40% 的城市间货物运输，输送量高于其他任何运输方式。约 20% 的货车运输的是对于电力部门至关重要的煤炭。每年有超过 2 000 万城市间旅行者使用铁路系统，还有 4 500 万乘客使用地铁和城铁运输。保护铁路资产是确保美国经济和旅客安全的关键。

#### (1) 铁路运输面临的挑战

我们国家的铁路系统广阔而复杂，有着无数个出入口。火车站在设计、结构和用途上的千差万别复杂化了该部门保护工作的总体框架。该部门的规模和牵涉的范围使有效和高效应对各种威胁变得非常困难。这种情况令保护工作陷于复杂之中，但同时也减少了恐怖袭击的某些潜在机会。例如，列车是在固定线路上行进的，具有极高的可控制性。当列车被劫持时，可以离开主线路，从而减轻威胁带来的危害。同样，桥梁或隧道遭袭可能会对沿途的主要运输线路造成影响，但是造成全国性破坏的机会毕竟十分有限。

与铁路运输相关的较大风险是危险材料。火车常常会运载其他部门和公众服务必需的危险材料。涉及危险材料运输的决策流程十分复杂，需要业界与政府密切协调。部门信息共享流程可以帮助预防采取过激的安全措施，如限制为应对地方性突发事件而采取禁止全国范围内运输危险材料这样的地毯式安全保护手段。

应对货物运输安全挑战的解决方案应该考虑到，在很多情况下，商品（如国家安全中的某些基本材料）的流动是必须得到保障的。窒息商品流动以达到满足安全要求的目的，只能是把安全威胁的一种后果转变成另外一种后果。当出现一种必然会令铁路运输中断的威胁时，可用以确保运营持续进行的完备流程便能够减轻无意中造成的负面影响。例如，保持运营正常的规划可以帮助确定如何快速恢复商品流动、变更线路是否可以用作一种保护手段或者哪些特殊物品的运输（如重要国防物资）应该特许通行。

另一个重要问题是要用特殊标记说明货柜车运输的是危险材料。在发生突发事件时，货柜

车上的明显标志可以帮助向应急响应人员示警正在运送的是危险货物。但是，设计者必须特别留意不要让示警标志系统轻易被恐怖分子识破。

与航空业一样，铁路业也要面对在持续高度戒备时期增加安全措施的额外成本。自“9·11”事件以来，全国各地的铁路部门一直在实施保护措施方面超负荷运转，以求能够满足当前威胁环境的安全要求，员工加班和招聘临时保安人员是无法避免的结局。这样的财力物力消耗还要继续下去。铁路部门不得不将这种高度戒备作为一种“常规”状态。有些现金羞涩的运营者不得不通过降低业务量来维持提供更高级别安全措施的平衡。

铁路部门拥有确保运营持续进行的完备流程和对调度、控制和通信设备的备份，足以应付地方性或小规模的破坏。建立这种可以确保突发事件后继续正常运转的备份系统存在着很大问题，因为这需要为规模巨大的结构性强化支付很高费用。

## （2）铁路运输安全保护方案

为了应对布满风险的环境，铁路业一直在与交通部积极合作。因此，它对本行业进行了全面的风险评估，同时建立了陆路运输信息共享和分析中心，用以推动与针对铁路的网络和物理威胁相关的信息的交流。

“9·11”事件以来，很多铁路运营者加大了对安全计划的投入。新增的铁路安全保护方案涉及以下几个方面的工作。

### ➤ 开发改良型危险材料运输决策标准

国土安全部和交通部将与其他联邦部门、州和地方政府以及业界共同开发一种经过改良的流程，以确保根据信息对危险材料运输做出决策。

### ➤ 开发与检查跨模式中转运输的货物或旅客行李相关的技术和规程

国土安全部和交通部将与业界相关机构共同确定和推动相关技术的开发，以确保跨模式中运输的货物的安全和对危险物品的检查。

国土安全部和交通部还将与铁路业共同开发或投用可以满足应急响应需要的危险材料标志系统，但要避免系统轻易被恐怖分子识破。

### ➤ 明确确定与浪涌要求相关的角色和责任

国土安全部和交通部将与业界共同确定基础设施保护的角色和责任，以使铁路业在发生灾难性事件时能够满足对资源的浪涌要求。

成本和资源配置依然是铁路业必须持续面对的一大问题。国土安全部和交通部还将组建一个由政府 and 业界代表组成的工作小组，负责选择可以满足浪涌要求的方案，其中包括在极端紧急情况下动用联邦设施和功能。

## 高速公路、卡车运输和客车运输

卡车和客车运输业是我国运输基础设施的一个基本组成部分。没有该部门的资源，人口、货物和服务在全国的流动会受到极大阻碍。卡车和客车运输业的基础设施包括高速公路、公路、跨模式中转枢纽、桥梁、隧道、卡车、公共汽车、维修设施和公路交界交叉路口。

### （1）高速公路、卡车运输和客车运输面临的挑战

由于规模和运营方式各异、所有者和运营者数量众多，卡车和客车运输业具有极高的韧性和灵活性，能够满足市场的各种需求。出于同一原因，这个部门被分割成很多个部分，由州和联邦政府（有时还有地方政府参与）分层管理。卡车和客车运输业的规模和广泛分布对其基础

设施的保护提出了严峻挑战。

运输瓶颈点（如桥梁和隧道、跨模式中转枢纽、交界交叉路口、高速公路出入口等）是行业独有的挑战。由于对基础设施瓶颈点的全面了解十分有限，确定关键瓶颈点的通用标准很难制定。我们必须对重要资产作全面和系统化确定，尤其是那些遭破坏或摧毁后会威胁到公众的健康和安全并会对经济造成巨大影响的重要资产。

虽然很多州对自己管辖的高速公路基础设施进行了风险评估，但却不存在反映真实情况的比较基础可用来确定基础设施的相对关键性。同样，也不存在对瓶颈点进行脆弱性评估的协调一致的机制，同时也没有对如何降低风险进行规划和对规划进行评估。部门内缺乏统一行动的一大主要原因是推动业内成员间交流信息和协调一致进行规划的资金奇缺。结果，业界既不全面了解本部门面临的风险，也没有用于制定保护规划的适宜安全标准。而且，该部门运营的多样性和广泛的分布使这种情况进一步复杂化了。

由于本部门小规模公共和私营所有者和运营者数量繁多，基础设施保护的成本也是一大挑战。像铁路业一样，新增安全投资除了要考虑财政因素外，高速公路、卡车和客车运输企业还把交界交叉路口因安全因素而出现运输延迟的可能性视为一大潜在经济问题。

该行业面临的另一挑战是在多部门管辖的情况下处理安全突发事件的方式。由于不同执法机关处理卡车盗窃等犯罪行为的方式各不相同，对安全突发事件的执法反应在不同管辖范围之间自然缺乏一致性。

#### （2）高速公路、卡车运输和客车运输保护方案

与其他主要运输业一样，高速公路、卡车和客车运输业也在“9·11”事件后对自己的安全计划进行了评估。然而，该行业规模庞大、运营多样的特性要求利益相关人之间必须进一步加强协调合作才能确保在全国范围内实施整体化的统一安全保护手段。此外，加强对系统的整体了解还会导致产生适应性更强、受入侵干扰更少、成本效益更高的安全流程。高速公路、卡车和客车运输安全保护方案涉及以下几个方面的工作。

##### ➤ 加强对风险、威胁和脆弱性的全面评估

国土安全部将与交通部和其他部门利益相关人密切合作，共同推动本部门的风险、威胁和脆弱性全面评估工作。

##### ➤ 为确定和减少瓶颈点制定指导方针和执行标准

国土安全部将与交通部和其他部门利益相关人密切合作，为确定和减少全国和地区性瓶颈点制定指南和标准。

##### ➤ 通过先进技术强化业内基础设施抵御恐怖袭击的能力

国土安全部将与业界以及州和地方政府共同开发和确定可以支持分析和提高反恐保护成本效益的潜在技术解决方案和标准。

##### ➤ 制定提高运输行业运营者安全意识的全国教育计划

国土安全部和交通部将与业界共同制定一项旨在提高运输行业运营者安全意识的全国教育计划，为这个高度多样化行业的成员之间更好的协调合作打下基础。

#### 管道

美国有一个庞大的管道业，管道长达数十万英里，其中大部分埋设在地下。这些管道线输送原油、提炼后的石油和天然气等各种产品。

管道业已经采取了一系列安全措施以应对附近地区发生灾难性事件带来的潜在影响。并且,大部分管道设施都可以通过快速修复或是改用其他线路来减轻损失。一个甚至是几个管道设施遭到破坏不会中断整个系统。总体而言,管道业有着很强的紧急情况处理和恢复能力,而且大部分大型操作控制中心都制定了综合性应急计划和备份协议。

#### (1) 管道业面临的挑战

尽管管道不是独立的实体,但它们却是工业和公共服务网络的整体组成部门。缺少了一段管道可能会对依赖可靠的燃料供应的各种设施和工厂造成影响。

数十万英里的管道遍布整个美国,期望将所有设施都置于万无一失的安全保护之下是不现实的。因此,保护工作必须侧重于这样一些基础设施:对它们的破坏会对能源市场乃至整个经济造成巨大影响。对于管道业而言,决定保护什么和什么时候对其保护是涉及基础设施保护工作成本效益的重要因素。在需求高峰期(如冬季),管道系统通常以最高负荷运转,因此对于那些依赖于管道服务的设施和功能更重要。

总体而言,管道业的安全记录良好,同时拥有危机发生时处理被破坏设施的管理协议。然而,管道输送的很多产品都是易爆物,因此对它们的保护是一个重要问题。

管道跨越诸多州和地区,有的甚至跨越了国界。利益相关人数量大、种类多,致使行业内涉及破坏事件发生后管理(尤其是对管道设施恢复输送能力的管理)、重建和快速恢复服务的规章或安全计划混乱不堪,有时甚至相互矛盾。

管道业与能源和电信部门之间日渐增加的互依赖性使得本行业与其他关键基础设施在制定保护和反应规划过程中相互合作变得极为必要。业界公司很难单独就其关键基础设施所受攻击产生的更为广泛的影响做出评估。这些互依赖性要求通过跨部门的协调合作来真正对涉及国家安全的问题担负起责任。此外,有些与恢复或重建相关的问题要求业界至少做出地区性规划,同时要求业界成员之间共享有可能涉及私人所有权的敏感商业信息。

#### (2) 管道业安全保护方案

在历史上,为了确保自己输送石油和天然气产品的能力,管道业内公司一直都是独自对设施的安全进行投资的。来自业内大公司的代表对当今这个充满恐怖主义风险的环境进行了分析研究,共同制定了一项行动计划,其中包括业内信息共享的内容。除了这些努力外,交通部还开发了一套确定管道设施关键性的方法,同时提出了一套与国土安全顾问系统威胁级别相对应的保护措施。新增的管道业安全保护方案涉及以下几个方面的工作:

##### ➤ 制定标准重建协议

国土安全部将与能源部、交通部和业界共同开展一项识别、明确和建立相应权力和规程的研究,用以在破坏事件发生后尽快重建设施。

##### ➤ 制定标准安全评估和威胁防范指南

国土安全部、能源部和交通部将与州和地方政府以及业界共同制定一项指南,用以指导管道业评估脆弱性、改进安全计划、实施防范威胁的保护行动以及升级反应和恢复计划等方面的工作。

##### ➤ 与其他部门共同控制产生于互依赖性的风险

国土安全部将与能源部和交通部共同建立跨部门工作小组,研究确定整体化保护重点和应急响应计划。

## 海运

海运基础设施包括港口及其附属资产、船只和旅客运输系统、海上和内陆水道、水坝、运河以及连接这些水上系统的铁路网和管道网。美国共有 361 个海港，它们的运营在规模和特点上有很大差别。

大部分港口都有各种水边设施，它们被不同的实体拥有、运营和使用。州和地方政府控制着一些港口设施，但是大部分设施是由私人拥有和运营的。绝大部分船只归私人拥有和运营。货物存储在港口的仓库中，被装到轮船和其他运输工具上，再由轮船和运输工具运送到全国各地。国防部还将一些商业海港指定为战略港口，为其为军事部署提供设施和服务。

### （1）海运面临的挑战

海运基础设施的规模、多样性和复杂性使得对进入港口的车辆和货物进行全面检查非常困难。当前使用的检查方法无论从物理还是从技术角度看，都十分匮乏并且成本很高。就像对其他跨越国界的运输方式一样，我们必须设法在高效处理货物和旅客与适度的安全保障之间达到平衡。

海运业的运营有很大一部分是国际性的，由国际协议和跨国机构管辖着，如国际海运组织等。与外国政府就海运规则和实践措施进行谈判是国务院的职责。这方面的国际谈判往往要耗费很多时间。

交通部最近提出了客轮和港口安全指南，其中包括乘客和行李检查以及人员培训等方面的内容。海运业需要就高成本效益的技术开展研发，以便迅速检查出易爆物和其他危险物品，以及改进船只设计，将船只遇到袭击时沉没的可能性降至最小。

港口系统的大部分成分都是对安全保护工作的严峻挑战，尤其是那些高风险货物。物理和操作安全指南已经在全面审定之中，交通部和国土安全部将通过这些指南对适宜的保护行动提出指导和建议。提高海运业安全水平的工作必须考虑归属多部门管辖并具有国际背景的基础设施。

### （2）海运业安全保护方案

“9·11”事件以后，所有港口都进行过初步风险评估。这些风险评估有助于确定关键基础设施和重要资产、评估脆弱性、制定减轻风险战略和阐明最佳实践措施。大部分港口当局和私营设施所有者也重新审查了自己的安全措施。根据这些初步风险评估，交通部增加了船只通报要求，以把有限的资源集中使用到对那些携带高风险货物和大量乘客的高风险船只航行的监控上。交通部和美国海岸警卫队还制定了一项“海上整顿”计划，并派遣海上治安队执行相关措施。

此外，交通部还参与了执行现行国际标准以及制定强化港口、船只和设施安全的标准的工作。交通部还与美国海关总署共同实施《集装箱安全方案》，以确保海上运输链的安全。不符合相关法规规定的货物在进入美国港口时会受到更加严格的检查，延迟到货在所难免。

新增的海运安全保护方案涉及以下几个方面的工作。

#### ➤ 确定脆弱性、互依赖性、最佳实践措施和补救要求

国土安全部和交通部将进行或更大范围地推动确定脆弱性和互依赖性的安全评估工作、推广最佳实践措施和就如何制定适宜的控制风险战略提出指导和建议。

#### ➤ 制定一项计划，实施与各种威胁级别相对应的安全措施

国土安全部和交通部将与其他联邦相关部门和机构、港口安全委员会以及私营设施所有者

和运营者密切合作，共同制定或推动制定安全计划，以将港口、船只和其他关键基础设施面临的风险降到最低程度。

➤ 制定加强海上运输监管和争取国际合作的流程

国土安全部和交通部将与其他联邦相关部门和机构、港口安全委员会、私营设施所有者和运营者以及外国政府、国际组织和商业机构密切合作，共同制定一套流程，用以确定装货港口所面临的潜在威胁并监控经确认驶往美国的船只、货物和乘客。

➤ 建立加强港口物理和运行安全的样板

国土安全部和交通部将与联邦相关部门和机构以及港口所有者和运营者共同建立用以加强港口物理和运行安全的样板。有关的指导可能包括工作人员身份识别措施、经过强化的港口设施设计、船只严格管理计划、国际集装箱密封标准、货物和船只防入侵安全和监控系统研发指南、集装箱实时追踪反馈信息、高风险货物预先甄别流程和恢复计划等。相关的行动将包括分析研究其他国家的最佳实践措施。

➤ 为货轮和客轮制定安全保护指南和技术要求

国土安全部和交通部将与国际海运组织和业界共同为货轮和客轮的安全研究和制定相关指南和技术要求。

➤ 改善水路安全

国土安全部和交通部将与州和地方政府所有者和运营者共同制定改善水路安全指南并确定必要的支持，如为水路运输开发电子监控系统、仿真识别和保护关键设施的船运系统以及确定定期水路巡逻的要求和流程。

## 公共运输

每年会有大约 95 亿人次使用公共运输工具出行。事实上，公共运输每天运送的乘客总量超过其他所有运输方式的总和。从“9·11”事件对航空运输的影响来看，对公共运输的恐怖袭击会产生巨大的地区性和全国性经济影响。

公共运输系统的设计是为大众提供便利的。大部分公共运输设施都归州和地方政府机构拥有并运营。城市可以依赖公共运输系统解决很大一部分就业问题，同时还能提供紧急状况下的疏散手段。因此，对公共运输的保护是我们的一项重要任务。

### （1）公共运输面临的挑战

公共运输归属多个机构管辖。这些机构必须相互交流和有效合作才能使公共运输系统形成一个整体而不是各自为战。公共运输的资金由地方政府提供，因此也由地方政府管理，是作为非营利实体运营的。联邦公交管理局在监管公交系统安全规划和运营方面缺乏足够的立法权。

公共运输系统的设计是开放式的，便于公众使用，而这使出入口的监控变得非常困难。保护这些出入口需要昂贵的费用。公交主管部门必须拥有足够的财政资源应对紧急情况和保持适宜的安全级别以阻止对广泛地理区域的攻击。满足新安全要求的成本会给业界带来重大的经济后果。

每个城市和地区都有独特的公共运输系统，它们在规模和设计上有着很大差别。不可能有任何安全保护计划或信息共享机制适合于所有公交系统。尽管存在着这样的差异，作为一种总体性规范，基本规划元素还是适用于各种系统的。

### （2）公共运输业安全保护方案

由于公共运输系统地理分布广泛、规模和设计各异，用于安全规划的识别关键性指南和标

准是统一公共运输安全保护行动的关键。公共运输合作研究计划委员会就预防、减少、防范和反应等方面提出了 10 个研究项目并监督项目的实施。这些建议为上述方面的规划工作给予了进一步的指导。

新增的公共运输业安全保护方案涉及以下几个方面的工作。

➤ 确定规划的关键方面和制定相关指导方针和标准

国土安全部将与交通部以及其他联邦、州和地方政府公共运输主管官员共同确定规划的关键方面并制定保护公共运输系统的适宜指南和标准。规划的这些关键方面以及指南包括设施、轨道和车辆的设计和工程标准、运营人员应急指导、操作人员筛选方法和培训计划、安全规划疏漏标准、相互援助策略和运营规划的持续性。

➤ 确定保护工作的障碍和实施强化安全措施

国土安全部将与交通部和业界代表共同研究相关法律、立法和法令权限，从而为公共运输系统建立一个总体保护框架，同时还确定实施必要安全强化措施所会遇到的障碍。

➤ 与其他部门合作，共同控制产生于互依赖性的风险

国土安全部将与交通部共同组建跨部门工作小组，负责在公共运输与其他关键基础设施相互依赖的情况下开发一体化保护重点以及应急响应计划模型。

## 银行与金融

银行与金融服务部门的基础设施包括各种物理结构（如建筑物和金融服务设施）和人力资本。该行业的大部分活动和操作都发生在大型商业写字楼中。需要保护的物理结构包括零售和批发银行服务、金融市场、市场监管机构和金融资产的物理存储设施。今天的金融服务，如支付和清算系统，大部分都实现了电子化，不过也会发生少数资产的物理转移。金融服务基础设施包括计算机之类的电子设备、存储设备和电信网络。该部门除了有上述重要物理成分外，很多金融服务员工掌握了高度专业化的技能，因此，这些人力资本也在该行业关键基础设施的基本组成部分之列。

金融业也依赖公众长期保持的信心以及他们对维持正常运转的参与。金融机构通常只将储户的一小部分资产以现金形式放在手边。如果众多储户和顾客同时取款的话，金融系统会面临巨大的现金流动压力。鉴于此，联邦监管机构采取了避免现金流动缺乏的防范措施。在危机和灾难时期，维持公众信心需要金融机构、金融市场和支付系统正常运转或快速恢复正常运转。

此外，在危机时期，财政部长、联邦储备委员会主席和证券交易委员会会主动发表声明，帮助解决公众的信心问题，就像“9·11”事件发生之后所做的那样。财政部、联邦和州的监管机构为银行与金融部门制定了应急交流计划。

在零售金融服务方面，物理资产在地理上分布极广。零售业的特点是可替代性很高，也就是说，在短期危机中，一种支付机制或资产很容易就会被另一种支付机制或资产所取代。例如，在零售市场上，消费者可以通过现金、支票或信用卡付账。

银行与金融服务业是被严格监管的，竞争非常激烈。业界专业人员和政府监管人员会定期确定部门脆弱性并采取相应的预防措施，其中包括制裁那些始终无法达到标准的金融机构。

### （1）银行与金融部门面临的挑战

与其他关键部门一样，银行与金融服务部门的持续正常运转依赖于几个关键基础设施行

业，如电力、运输和公共安全服务。该部门还特别依赖计算机网络和电信系统来确保服务的正常进行。这些系统遭到破坏的可能性是值得关注的重要问题。例如，“9·11”恐怖袭击之后，股票市场关闭了4个交易日，这不是因为股票交易系统无法使用，而是因为曼哈顿下城的电信中断且不能立即恢复。作为减轻损失的一种办法，金融机构对其系统和运作设置了备用和备份。

多个职能重叠的联邦情报机构负责发布有关袭击威胁的信息，从而给业界和政府带来了混乱并使工作重复。财政部建立了金融和银行信息基础设施委员会，作为关键基础设施保护总统委员会的执行机构。金融和银行基础设施委员会由来自13个联邦和州的金融监管机构的代表组成<sup>①</sup>。该委员会现在正与国家基础设施保护中心、金融服务信息和共享中心以及国土安全办公室合作，共同改进信息发布和共享流程。

## （2）银行与金融部门安全保护方案

9月11日对纽约市的恐怖袭击表明我们的金融服务行业有着很强的抗袭击能力。行业的强大保护和备份系统在危机中都能正常运转。从1998年起，该部门一直在与财政部合作，通过组织严密的安排使自己能够应对威胁越来越大的环境带来的风险，尤其是网络攻击。

大多数金融机构都在继续评估其安全系统。“9·11”恐怖袭击之后，金融行业进行了全面的系统安全评估，同时制定了系统恢复计划。作为一个整体，该行业在财政部的支持下开始了全行业的风险评估。此外，金融机构还各自对其安全系统增加了投资。

新增的银行与金融部门安全保护方案涉及以下几个方面的工作。

### ①确定和解决部门对电子网络和电信服务的依赖性风险

金融服务部门对信息系统和网络的高度依赖给本部门带来了很多问题。财政部将与国土安全部共同组建一个由电信和金融服务部门以及其他联邦机构代表组成的工作小组，负责研究和解决由于本部门依赖电子网络和电信服务而带来的风险。

### ②加强安全信息的交流

国土安全部将与财政部、金融和银行信息基础设施委员会、金融服务信息共享和分析中心密切合作，加强联邦政府与部门成员之间的信息交流，强化信息共享机制，使威胁信息在日常和出现突发事件的情况下都能顺利交流。

## 化学工业和危险原料

化学工业提供了美国经济和生活标准离不开的产品，制造了其他行业需要的基本产品。例如，化学工业为农业生产化肥，为水净化行业生产氯气。此外，化学工业每年还生产970多亿美元的医疗保健药品。

现在，化学工业是我国最大的出口行业，约占我国总出口的10%。化学工业还是我国最具创新精神的行业，拥有我国全部专利的七分之一。这也是我国的化学工业能够在国际化工市场上保持竞争力的主要原因。

化学工业在公司规模、地理分布上存在着很大差异。化学工业的产品和服务依赖于原材料、制造工厂和加工工厂、配送系统以及研究设施和支持设施（如运输和电力产品）。

① 金融和银行信息基础设施委员会由联邦和州的金融监管机构的代表组成，其中包括期货交易委员会、州立银行监管人联合会、联邦储蓄保险公司、联邦住屋融资局、纽约联邦储蓄银行、联邦储蓄委员会、全国保险专员协会、全国信用合作社管理局、通货监理局、联邦住房企业监管办公室、国土安全办公室和网络安全办公室、节约监督办公室和证券交易委员会。



公众的信心是化学工业持续发展的一个重要因素。产品安全的不确定性对生产者和使用者都有巨大的影响。在安全生产方面，很多联邦法律都有降低事故发生率的规定。但是，现在还没有一个职能明确的联邦监管机构帮助为化工设施确定全面和统一的标准。

如果化学工业受到恐怖袭击，除了经济损失之外，公共卫生和公众安全也会受到影响<sup>①</sup>。因此，降低化学工业的对恐怖袭击的脆弱性是确保经济平稳运行以及公民和环境安全的重要因素。

#### （1）化学工业和危险原料面临的挑战

足够的供给对化学产品的下游用户来说非常重要。很多大型市政水处理设施仅仅库存用以消毒几天用水量的氯气。农业化工产品，尤其是化肥，必须在短时期内大量使用。一些化工产品不能以多种方式运输，因此会影响这些产品的及时运送。

化学工业的安全保卫能力和确保库存化工物品安全的能力至关重要。由于化工产品对于很多行业来说都是必不可少的，关键性化工产品的库存污染可能会对很多行业造成影响，甚至会影响公众健康和经济运行。另外，很多化工产品是有毒的，会对公共卫生和公众安全产生危害。加强化学工业的安全可能会大幅度增加成本，但也有一些成本较低的方式。不幸的是，由于化工厂在技术、产品、设计和工艺上千差万别，它们面临的风险也是各不相同的。因此，没有一个通用的安全标准可以适用于所有化学工业设施。

很多与化学工业相关的现行法律都是几十年前制定的，它们对于监测和控制有毒物品可能已经不再那么有效。例如，尽管农药销售商只能将农药卖给有执照的购买者，但是这些执照的获取非常容易。另外，各州发放执照的规定也不一样。

与其他大部分行业一样，化学工业也依赖其他行业的关键基础设施。例如，化学工业是我国第三大电力消费行业。

#### （2）化学工业和危险原料安全保护方案

当前，部分业内机构已经主动采取了积极措施来保护本行业的基础设施。例如，一些贸易协会已经制定了或是正在制定行业安全规范<sup>②</sup>，以帮助成员认识降低安全脆弱性的需要。这些值得称赞的努力会对化学工业和危险原料的保护工作产生巨大影响。这些措施只是刚刚开始执行。但是还有很大一部分运营主要化学设施的公司并没有遵守这些自愿性安全规范。

化学工业和危险原料安全保护方案涉及以下几个方面的工作。

##### ①提高设施的安全性

国土安全部和环境保护局将与国会共同提出立法法案，要求对化学设施，尤其是那些大量处理危险原料和位于城市附近的设施，进行安全脆弱性评估，并采取必要措施来降低这些安全脆弱性。

##### ②研究有关农药以及其他有毒物品出售和配送的现行法律规定

环境保护局将与国土安全部、其他联邦、州和地方政府机构以及其他利益相关人共同研究有关有毒物品和化工产品出售和配送的现行法律规定。这一过程将有助于确定是否有必要增加新的措施来解决与这些产品相关的安全问题。

##### ③继续发展化学工业信息共享和分析中心，吸收新的业界成员参加

① 化学工业和危险原料的具体基础设施可能应在“重要资产”中下明确定义，但是，由于它们的保护问题与整个行业直接相关，因此在本章进行讨论。

② 如美国化学联合会的管理方式责任制安全规范。

化学工业信息共享和分析中心旨在便利安全威胁的提前预警和共享其他与安全有关的数据信息。国土安全部和环境保护局将与业界官员共同在全行业推广信息共享和分析中心，以使所有业内企业全部加入该中心。

### 邮政和递送

美国人高度依赖邮政和递送。我们每天都会通过美国邮政系统邮寄将近 7 亿封信；30 多个城市和乡村邮政局每天会向 1.37 亿个地址递送信件。总体来说，美国邮政局运行的巨大网络包括在华盛顿的总部、遍布全国的上万个邮政设施以及和数十万个信件邮递点。美国邮政局在全国雇用了 74.9 万多名全职工作人员，每年的收入超过 600 亿美元。美国邮政局和私营邮寄公司每年总的营业额在 2 000 亿美元以上。

邮政系统高度依赖其他关键基础设施系统。美国邮政局使用的运输工具由邮政局自己拥有和向私人租用的车辆和设备组成。邮政局每天还使用商用飞机、卡车、铁路和船只运输信件。由于存在这样的依赖性，美国各地的很多重要邮政设施是与其他机构公用的。

全国邮政设施网络的多样性给安全保卫工作带来了严峻的直接挑战。此外，这个系统的总体规模和普遍性极容易被恶意攻击产生潜在的附带效应。2001 年秋天的炭疽疫攻击更加突出了这个问题。除了美国各地的邮件处理工作均陷于停顿外，带炭疽疫病毒的邮件引起了公众的广泛焦虑，转而造成了巨大的经济损失。

从历史上看，美国公众对邮政系统有着很强的信心和依赖性。当公众认为自己的健康和安全可能会被邮件影响的时候，这种信心会大大降低。因此，美国邮政局一直把着重点放在邮政部门所面临的特殊安全保卫问题上，并且在努力寻找适当的解决方案来加强邮政系统的安全性。

#### (1) 邮政和递送部门面临的挑战

本节所述保护挑战和方案与美国邮政局采取的行动密切相关。商业邮政和递送公司正在重组为一个部门，从而得以在行业内更为具体地确定和解决安全问题。美国邮政局已经与很多行业内的公司进行了合作，来共同解决攻击基础设施的保护问题。但是，我们还应该在这个领域内采取更多的行动。在美国邮政局的协助下，国土安全部将促使行业内主要公司进行对话，以解决整个行业关键资产保护问题。

美国邮政局确定邮政系统中需要关注以下五个方面：

- 主要设施的入口和位置；
- 邮件的经手过程；
- 独特的宪法和法律问题；
- 部门之间的合作；
- 对紧急状况的快速反应能力。

邮政系统的众多入口加大了保护邮政行业的难度。并且，这些入口散布于全国各地，这更加复杂化了安全保卫的问题。美国邮政局正在考虑采用具有高成本效益特点的邮件扫描技术，以此来对潜在危险发出早期预警。

很多关键性邮政服务设施的位置也加大了风险管理的挑战性。美国邮政局的几个主要设施都与其他政府部门公用，或是位于重要运输枢纽地带。搬迁这些设施通常会超出财政承受能力。

另一个影响邮政安全的因素是，邮件在运输过程中，并非总是处于邮政局的控制之下。通常，独立承包商会负责运输邮政局的邮件。由于邮政局使用了上百个远程运输公司，邮件会在运送过程中不断进入和离开邮政局的控制。为了解决这个问题，美国邮政局的运输合同要求所

有运输承包商及其工作人员必须接受犯罪和毒品背景审查，内容包括指纹和邮政检查部门的其他查询。

美国邮政局的安全努力面临着独特的宪法和法律挑战。具体来说，宪法第四修正案禁止不合理的邮件检查，因此，邮政局需要证明邮件扫描或 X 光检查的必要性。另外，一些公司不愿意开发和出售高科技扫描系统，因为他们担心自己会因为没被发现潜在威胁而承担责任。2002 年《有效利用科技手段反对恐怖主义法》（2002 年《国土安全法》的组成部分）减少了反恐仪器生产者对其产品的责任，从而大大降低了这样的风险。

## （2）邮政和递送部门安全保护方案

国土安全部将与私营递送和邮件邮寄公司合作，将这些实体的安全保卫问题统一到整个行业的基础设施保护工作中。

此外，美国邮政局在其紧急情况防范计划中提出了六个核心方案：预防、保护和减小健康风险、检测和识别、干预、清除污染和调查。以下是支持这些方案的重要行动的具体方面。

### ①提高保护和反应能力

国土安全部将与美国邮政局共同制定规划，增加突发事件应急响应（尤其是化学、生物和放射性污染）所需的备用设备和物资储备。国土安全部和美国邮政局还将分析研究需要大规模生产某些物资的需求。

国土安全部和美国邮政局还将与其他联邦部门、州和地方政府合作，共同协调并制定避免风险和控制风险的措施，同时为突发事件反应和补救制定统一协议。

### ②确保国际邮件的安全

国土安全部和美国邮政局将与相关机构一起分清国际邮件进入和离开美国边境时各部门所应承担的安全责任（如美国邮政局和美国海关）。

### ③推动和支持业内成员参加信息共享和分析中心

国土安全部将推动邮政和递送部门的成员加入相关信息共享体系。这个体系必须包括参与邮件、私人包裹和大型货物的航空和陆路邮递工作的政府和私营部门重要利益相关人。

### ④加强对关键设施的风险分析

国土安全部、美国邮政局和美国邮政检查局将对坐落于其他高风险设施之内、需要更全面风险分析的邮政设施进行评估。这些更加严格的必须考虑恐怖分子的能力和动机以及设施脆弱性的评估，可以为迁移高风险邮政设施提供判断依据。

### ⑤提高确认顾客身份及其与邮件关系的能力

美国邮政局将建立机制，在邮件投递点实施顾客身份及其与邮件关系确认措施，同时改进针对危险物品的不具侵犯性的被动式包裹检查系统。

### ⑥确认并协调与其他政府部门之间的冲突

国土安全部、美国邮政局和司法部将与州和地方政府合作，确认和解决联邦、州和地方法律规定之间的冲突，以确保邮政局对紧急情况的快速反应能力。

## 7. 保护国家重要资产

国家重要资产包括很多独特的设施、场所和建筑。这些设施、场所和建筑结构遭到破坏或被摧毁会在各个方面产生巨大影响。其中一类重要资产由各种代表着我们国家遗产、传统和价值的国家纪念碑和标志性建筑物组成。它们包括各种场所和建筑，如历史名胜风景区、纪念碑、

文化标志以及政府中心和商业中心。这类重要资产的场所和建筑通常会吸引大量游客和媒体关注，从而给保护工作带来了特殊的挑战。

第二类重要资产包括代表我国经济实力和技术进步的设施和建筑。在这些设施和结构里储存着日常生产需要使用的大量危险物资和化工产品。这些设施遭到破坏会对公共卫生、公众安全和公众信心以及经济带来严重后果。

第三类重要资产包括那些著名的商业中心、办公写字楼和体育场馆。这些地方通常会有大量人群来往。鉴于这些场所的全国知名度以及破坏所可能造成的人员伤亡，对它们进行保护是减少伤亡人数和维持公众信心的关键所在。

## 国家纪念碑和国家标志

### （1）国家纪念碑和国家标志面临的挑战

我们的国家纪念碑和国家标志带来了特殊的挑战，因为对它们的保护通常需要联邦、州和地方政府以及私营部门的全力合作。劳力、资源和责任往往很难划分。

保护我们的国家纪念碑和国际标志不受恐怖分子攻击，需要制定和协调全面政策、实践措施和保护措施。我们同时也面临着平衡游客访问和保护游客以及资产安全的任务。通常来说，保护资产的安全会限制游客对一些地区的游览和避免大量游客流动。

内务部是负责国家纪念碑和国家标志安全的主要联邦部门。内务部肩负着多重责任，包括对各种潜在袭击目标的保护。这些保护工作在举行国家庆祝活动时显得尤为重要。因此，内务部必须与各级执法机关和直接负责情报收集和国土安全的机构协调合作。

内务部及其州、地方政府和私营部门的相关机构还在招募、培训和维持强大安全保护队伍方面面临着独特的挑战。鉴于需要对很多潜在攻击目标（如国家公园、纪念碑和历史建筑）进行保护，维持强大、熟练的安全保护队伍是当前工作的重中之重。

### （2）国家纪念碑和国家标志安全保护方案

为了应对保护国家纪念碑和国家标志所面临的挑战，我们将在以下几个方面采取行动。

#### ①定义国家纪念碑和国家标志的关键性标准

内务部将与国土安全部共同制定具体指南，用以定义确定国家纪念碑和国家标志的关键性和保护重点的标准。

#### ②评估威胁和脆弱性

内务部将与国土安全部和其他相关部门共同对威胁和脆弱性进行评估，以确定游客保护流程和资产保护流程存在哪些差距。

#### ③维持高素质安全保护队伍

内务部将通过各种选择方案招募、培训和维持一支技术熟练和士气高昂的安全保护队伍。

#### ④实施以安全为中心的公众知情和提高公众安全意识计划

内务部将通过持续实施公众知情和提高公众安全意识计划寻求公众对国家标志保护工作的支持。

⑤与州和地方政府以及私营部门合作，确保不属联邦政府管辖的国家标志保护工作顺利进行

内务部将与州和地方政府以及私营机构共同制定选择方案，确保历史建筑、纪念碑等不属联邦政府管辖的国家标志的安全。

⑥使用创新性科技手段

内务部将与国土安全部和其他重要利益相关人共同探索以何种方式使用新科技手段确保游览纪念碑和其他名胜的游客的安全。

⑦规定重大活动必须增强安全措施

内务部将与其他执法机关共同确保重大庆祝活动和其他庆典中资产和游客的安全。

## 核电站

核电占我国发电总量的 20%。美国在 31 个州内建有 104 个商用核反应堆。近 25 年来，联邦监管机构要求这些设施维持严格的安全系统以抵御可能的攻击。核电站也是国内最坚固的设施之一。它们能够经受飓风、台风和地震这样的严重危险事件。这些核电站的强化设计包括防护墙、备用安全系统和被严密保护的废料存储系统。

“9·11”事件以后，我们大大加强了核电站的安全保卫工作。所有核电站都处于全天候戒备之中。并且，我们采取了具体措施来加强安全系统，以防止和减轻放射性物质泄漏的危害。我们还改进了监视系统，进一步限制人员的进入，同时还加强了与执法部门和军事部门的合作。除了这些强化措施外，所有核电站都有严格的安全和紧急情况应对计划，以进一步确保公共卫生和公众安全安然无恙。

### （1）核电站面临的挑战

损失一个核电站的发电量对全国电网的电力输送影响不会很大。但是，恐怖分子对任何核设施的袭击都将是严重的安全事件。核设施遭袭可能会引起放射性材料泄漏。即使放射性材料没有泄漏，公众对核设施泄漏的错误理解也会造成严重的负面影响。

国家放射性物质委员会目前正在对核电站进行周密的设计基础威胁和脆弱性分析研究，以发现安全脆弱性和提高安全水平。其他谨慎的安全措施也应在考虑之中，用以加强这些设施的防卫力量。

### （2）核电站安全保护方案

为了克服保护工作中遇到的挑战，我们将采取以下行动。

#### ①协调标准化脆弱性和风险评估工作

国家放射性物质委员和国土安全部将与核电站的所有者和运营者共同开发一直标准方法，用以对脆弱性和风险做出评估。

#### ②确定统一流程和确定保护核电站所需的资源

国家放射性物质委员和国土安全部将与核电站所有者和运营者以及地方、州和联邦机构合作，共同建立核电站在高度戒备期间和威胁迫近时要求外部安全力量增援的标准流程。

#### ③确定未经授权携带武器或爆炸物进入核设施为犯罪

国家放射性物质委员和国土安全部将寻求立法，把未经授权携带武器或爆炸物进入核电站认定为联邦刑事犯罪。

#### ④加强核电站的安全保卫力量

国家放射性物质委员和国土安全部将寻求立法，以允许核电站安全人员携带威力更大的武器。国家放射性物质委员和国土安全部还将帮助业界对私营企业安全人员进行培训，传授反恐技巧。

#### ⑤寻求将核设施列入反破坏法保护

国家放射性物质委员和国土安全部将寻求立法，将联邦反破坏法应用于核设施以及其运营者。

#### ⑥提高公众意识

国家放射性物质委员和国土安全部将与核电站所有者和运营者以及州和地方政府相关部门共同提高公众对核电站安全的认识以及对紧急情况反应速度。

### 水坝

有些规模较大、象征意义较强的水坝是我国关键基础设施系统的主要组成部分之一。这些水坝向大量人口、城市以及农业设施提供水源和电力。《国家水坝目录》列有约 8 万多个水坝。其中大部分水坝是小型的，而小型水坝的损坏不至于引起严重的财产损失或生命损失。联邦政府管理着大约 10% 的大型水坝，而这些大型水坝的损坏却会引起非常严重的财产损失或是对公共卫生和公共安全带来严重后果。其余水坝归属州和地方政府、公用事业单位或公司和私人所有。

#### (1) 水坝面临的挑战

在现行法律政策下，水坝所有者要负责水坝的安全。所以，保护水坝安全的资源在不同种类的水坝中差别很大。并且，种类繁多的水坝所有权大大复杂化了对水坝损坏的不良后果进行有效评估。鉴于这些现实，开发出一套更全面的风险评估和风险管理机制是我们的当务之急。

#### (2) 水坝安全保护方案

为了克服水坝保护工作中遇到的各种挑战，我们必须在以下几个方面采取行动。

##### ①开发水坝风险评估方法

国土安全部将与联邦、州和地方政府相关部门的代表以及私营水坝所有者共同设计评估水坝风险的方法，并且制定相关标准，用以在《国家水坝目录》中确定需要加强评估和保护工作的重点。

##### ②制定保护行动方案

国土安全部将与其他相关政府部门和机构共同组建一个跨政府部门的工作小组，对保护国家关键水坝的行动做出规划。

##### ③建立部门信息共享和分析中心

国土安全部将与其他相关公共-私营部门实体共同建立一个水坝信息交流和预警体系，其结构与其他关键基础设施部门的信息共享和分析中心类似。

##### ④制定全国水坝安全保护计划

国土安全部将与其他相关部门和机构（如国家水坝安全协会、美国水坝协会等）共同制定全国水坝安全保护计划。

##### ⑤制定应急响应方案

国土安全部将与其他相关部门和机构共同确定那些会因关键水坝损坏而受影响的下游地区，同时制定相应的人口和基础设施保护以及应急响应方案。

##### ⑥开发可提供保护解决方案的技术

国土安全部将与其他相关部门和机构共同为水坝开发新的保护技术方案。新技术方案应能确定和减轻与水相关的威胁。例如，新技术方案可能涉及设置感应器、障碍物和通信系统，以减少未经授权船只和装置进入水坝关键区域的可能性。

### 政府设施

“9·11”事件以前，对政府建筑的主要威胁是使用爆炸物。1995 年发生俄克拉何马城联

邦大楼爆炸案之后，国内的很多大型政府中心楼群都采取了防护措施来保护主要物理财产，如设置水泥障碍物、加强监视系统、提高停车场限制等。虽然爆炸物仍旧是很大的安全隐患，但是基地组织的袭击给美国政府的设施带来了新的威胁。

综合服务管理局是管理联邦政府设施的主要负责机构。另外，国防部和退伍军人事务部也管理着部分联邦政府设施。联邦政府设施包括归联邦拥有的设施和联邦政府从私营部门租借的设施。综合服务管理局负责与其他部门合作，共同评估联邦设施面对各种袭击威胁的安全性。将要划归国土安全部的联邦保护局需要通过与设施内的各政府部门以及私营部门合作来制定和实施相应的安全措施。

### （1）政府设施面临的挑战

大部分政府机构与很多非政府机构共同使用同一建筑物，如商店、饭店等。联邦法律和规定适用于联邦拥有的建筑。但是在私人拥有的建筑里，联邦法律和规定仅能应用于联邦机构使用的区域。例如，联邦法律禁止非法携带武器进入联邦建筑，但是在私人拥有的建筑里，这个规定只适用于联邦机构使用的区域。这些建筑的私人所有者可能不会修改他们的规定来适应联邦的高安全保卫需要，如在大厅中安装监视装置、重新设计入口处以限制人员流动或是在入口处安装 X 光仪器和金属探测仪器等。在安全和公众隐私权之间达到平衡的需要提出了更大的挑战。

### （2）政府设施安全保护方案

为了克服保护政府设施面临的挑战，我们将采取以下行动。

#### ①制定相关流程，用以在联邦机构租用的私人设施中区分非联邦租户和访问人员

国土安全部、综合服务管理局和其他联邦部门和机构将与私营部门房地产协会共同设计出一套不侵犯隐私权的区分人员流程。

#### ②确定政府设施的关键性和脆弱性

国土安全部、综合服务管理局以及其他联邦部门和机构将与联邦政府租用设施的所有者共同开发一种用以确定政府设施关键性和安全脆弱性的标准方法。

#### ③为需要采取专门安全措施的设施制定长期建筑标准

国家标准局、国土安全部以及其他联邦部门将继续努力为需要防爆炸和其他专门安全措施的设施制定长期建筑标准。

#### ④在联邦租用设施中使用新技术安全措施

国家标准计量局、国土安全部以及其他联邦部门和机构将与私人所有者共同试验使用新技术安全措施来提高安全保卫水平（如感应器系统等）。

## 商业重要资产

保护重要商业中心、写字楼、体育场馆、主题公园以及其他有大量人群汇集的场所是我们面临的主要挑战之一。对这些场所的日常保护是其所有者和运营者以及当地执法部门的责任。

联邦政府对这些商业重要资产保护的责任是间接的，其中涉及时提供恐怖袭击风险提示和警报，以及与商业企业共同协调各设施安全流程，使之与国土安全顾问系统的各个警报级别相吻合。此外，向那些负责制定建筑物建造、行业标准的机构提供支持和技术援助也是联邦政府的一项重要任务。

联邦政府通常只是在有重要任务来访或要举行指定的国家安全特殊活动时才会对商业设施协调或提供物理安全保护。由于国家级人物的造访以及重要商业场所和设施所可能带来的人

员和经济后果，政府与商务部门通力合作，共同确保我国重要商业中心和人群聚集场所的安全，是至关重要的。

#### （1）重要商业资产面临的挑战

恐怖分子袭击商业设施或活动场所的可能性很难确定。可能的恐怖袭击手段有很多种，从常规爆炸物到大规模杀伤性武器都有可能。每个商业设施面对不同袭击手段的脆弱性各不相同，是由该设施的设计、工程、规模、使用年限、用途和内在住户综合决定的。不同地区、不同行业、不同所有者的建筑标准、设计标准和安全标准也是都各不一样。最重要的是，商业设施的所有者和运营者必须对其设施的脆弱性做出评估，并采取措施减轻其受攻击时所产生的破坏影响。

#### （2）重要商业资产安全保护方案

没有哪种具体行动能够一举消除由恐怖分子蓄意袭击重要商业设施或活动场所的威胁带来的全部潜在风险。然而有些措施却可以通过使恐怖分子策划和实施袭击过于复杂而降低他们将商业设施作为袭击目标的可能。

例如，减小商业设施面对爆炸物或化学、生物和放射性物质攻击的脆弱性，要求使用一套全面的方法。其中，第一步是要在设施及其附属系统（如供暖、通风和空调系统）的工程设计中考虑潜在恐怖袭击的可能性。

第二步是对可以阻止或限制恐怖分子进入设施及其关键节点的物理安全设计特点、系统、流程和规程作全面评估。防止恐怖分子进入目标设施要求在入口、仓储区、维修区、屋顶采取适宜的安全保护措施，同时还要严防恐怖分子从供暖、通风和空调系统的室外入口点进入设施。

第三步是对供暖、通风和空调系统及其部件进行内部评估。这一步要侧重于评估这些设备作为化学、生物和放射性物品攻击导体的脆弱性。所涉关键区域有供暖、通风、空调系统控制总台、空气流通方式、空气压力、空气过滤和净化能力以及可能的泄漏物。如果这些系统所经过的设计、安装和维护是正确的，空气过滤和净化系统能够大大减轻化学、生物和放射性物品攻击的危害性。

最后一步涉及制定和演练突发事件应对计划，其中应该把最可能和最糟糕的物理安全破坏、飞机撞击、传统炸药雷管以及化学、生物和放射性物质释放等所有情况都考虑进去。这个最后的重要步骤必须包括建立与地方执法部门和应急响应人员相互协调合作的流程和系统。

为了加强对重要商业场所和设施的保护，使之不受恐怖袭击之害，我们将采取以下行动。

##### ①与私营部门共同执行联邦建筑物安全标准和实践措施

国土安全部、综合服务管理局、国家标准计量局以及其他联邦部门和机构共同将制定一套计划，以便与私营商业设施所有者和运营者共同执行联邦建筑物安全标准，脆弱性和风险评估方法、实践措施和技术解决方案（如物理障碍、闭路电视、入侵物探测装置、化学、生物和放射性物质探测装置、爆炸物探测装置等）。

##### ②加强威胁信息的有效发布

国土安全部将与情报和执法部门共同寻求和摸索及时向商业设施所有者和运营者发布威胁提示和警报信息的流程和系统。

##### ③实施国土安全顾问系统

国土安全部将与商业设施所有者和运营者密切合作，将国土安全顾问系统的具体保护措施和流程结合到商业设施的安全保护工作中。

##### ④探索鼓励实施强化安全设计或安全措施的选择方案



国土安全部将对鼓励选择方案进行探索，以奖励那些在设施设计中采用了具体安全措施的商业设施所有者和运营者，或者那些采用了具体流程、规程和技术检测、预防或减轻恐怖袭击后果的商业实施所有者和运营者。

#### ⑤改进私营商业设施建筑规范

国家标准计量局将制定一套全面的私营商业设施建筑规范，以进一步确保建筑物的安全，减小建筑物倒塌的可能性并增加其对高温燃烧的抵抗度。

## 8. 总结

保护我们国家的关键基础设施和重要资产是国土安全的核心任务。这部国家战略再一次明确了我们作为一个国家保护关键基础设施和重要资产不受恐怖袭击的决心。

当我们开始应对那无数挑战的时候，我们必须牢记需要保护的基础设施和资产的复杂本质。作为袭击的潜在目标，我国的关键基础设施和重要资产是由多种相互依赖的设施、系统和功能交织在一起的混合体。在这些关键基础设施和重要资产中，政府只拥有和运营其中的一小部分，而大部分是由私营部门控制的。所有这些基础设施和资产都在某种程度上面临着恐怖袭击的威胁。

这些关键基础设施和重要资产是一个真正的“系统的系统”。对一个资产或一个基础设施保护的失败会产生对其他基础设施和资产保护失败的连锁反应。这种连锁反应可能会带来更严重的后果，从而影响政府运作、经济稳定、公共卫生、公众安全、国家安全和公众信心。总而言之，当我们执行这个国家战略计划时，我们必须对事情的复杂性有充分的认识。

在本文中我们主要强调了我们国家的保护计划所面临的各种各样的挑战。我们制定了一个详细的日程表，从而使我们得以基于威胁、脆弱性和风险来确定并直接解决那些最迫切的问题。但这只是漫漫征途的一个开始。

当我们开始的时候，必须同样牢记我们面对的本质的对手。9月11日对世贸中心和五角大楼的恐怖袭击突出显示了我们在国家层面上的脆弱性，同时表明我们面对的是一个狡猾、具有高度适应性、耐心和机动性的敌人。“9·11”恐怖袭击也显示了敌人的决心、经验以及恐怖分子推行他们事业的不辞辛苦的精神。

我们不再假设恐怖分子不可能在我们的国土和基础设施基地上进行毁灭性攻击。事实上，考虑到恐怖分子的创造力和适应性，我们可以预期未来的攻击会在容量上和协调性上更加复杂。具有讽刺意味的是，我们自由社会的本质极大地便利了恐怖分子的行动，同时也阻碍了我们预测、防止恐怖分子行动和减轻其后果的能力。考虑到这些事实，实行本文列出的综合性国家保护战略就成为我们目前最迫切的任务。

本文第5章“跨部门安全优先级”中所列问题和行动方案是近期的国家重点。它们集中体现了那些会对我们政府、社会和经济的重要部门产生重大影响的障碍。对这些问题的潜在解决方案，如信息共享、威胁程度警报等，一旦实施，会极大地提高整个国家的关键基础设施和重要资产保护的总体水平。

这些行动领域，包括迅速确定和保护国家关键基础设施，以及开发出适宜的预警流程和系统，并保护受到威胁的具体资产，这些是联邦政府关键基础设施和重要资产保护工作的近期中心内容。因此，国土安全部和其他相关联邦部门将制定出详细实施计划，用以支持本文所列跨部门和部门特有的重点保护问题。

我们在改进和实施重点保护计划的过程中，必须牢记本文所列的指导方针。我们的努力必须首先确保公共卫生、公众安全以及政府和经济重要部门的安全运作并维持公众信心。要想实现这一目标，我们就必须明确职能和责任、加强透明度、建立各相关部门和人员相互协调的合作机制。

我们同时必须建立和扶植各级政府以及政府与私营部门之间的合作关系。这种公共-私营部门之间的合作关系应该建立在双向交流以及有关关键基础设施和重要资产保护的信息的及时交流上。这种合作关系同样应该扩展到研发和利用尖端技术解决普遍存在的保护问题上。共同的努力还应该包括发展和共享建模和仿真能力，以使公共-私营部门之间的决策支持和相互分析支持成为可能。

恐怖分子不尊重国际边境，他们不会被国际边境所限。因此，我们必须通过与墨西哥、加拿大以及所有友好国家的合作来保护我们的关键基础设施和重要资产。最后，我们在消除那些保护工作中遇到的障碍的时候，还必须捍卫我们这个伟大国家的标志——基本宪法自由。

联邦各部门、州和地方政府以及私营部门所有者和运营者在他们各自控制的关键基础设施和重要资产的保护工作中已经取得了很大的成绩。“9·11”事件后，我们的国内保护环境充满了浓烈的合作精神和巨大的急迫感。我们已经走过了很长一段道路，但更长的路还在前面。现在我们必须共同行动，以各级政府内和政府外有闯劲的领导作风，在共同合作的基础上执行本文所列的行动方案。

我们所希望的终点是成功地保护我们的最关键的基础设施和最重要的资产，适时地示警和保护那些面临迫在眉睫威胁的关键基础设施和资产，以及建立一个所有相关部门和个人都可以成功和有效执行各自保护任务的合作环境。前面的道路会充满惊险和挑战，所以我们不能犯任何错误。如果统一我们的路径和方法，我们就可以克服任何挑战，从而成功地保护我们的关键基础设施和重要资产。

---

## 八、工业界对国家战略的响应纲要（摘要）

关键基础设施安全合作组织（PCIS）

2002 年 7 月

---



扫二维码阅读全文

本文对应于《保护网络空间的国家战略》中“行动计划”的第3级“关键部门”中的私营部门以及非联邦的公共基础设施部门。

## 1. 目的

工业界的战略纲要包括了关键基础设施部门对《保护网络空间的国家战略》的贡献。保护我们的关键基础设施并不只是政府自己的事情，私营部门拥有并且运营着大量的关键基础设施，只有通过前所未有的公共-私营合作联盟，保护我们的国家和经济利益的共同目标才能得以实现。最初，关键基础设施包括银行与金融（金融服务）、信息与通信（I&C）、电力、运输、石油和天然气、供水、应急服务以及关键的政府功能，现在应急服务在国家战略中被划入了州和地方政府部门。

上述的每个关键基础设施部门都制定了自己的战略，描述了各关键基础设施工业为确保其关键服务的可用性而正在实施的行动。这些战略对正常运转所依赖的物理和信息基础设施做了同步的考虑，并指出了各部门对国家安全的贡献。第3章“介绍”由关键基础设施安全合作组织（PCIS）撰写，它覆盖了所有关键基础设施部门面对的共同问题。PCIS是一个建立于1999年12月的非营利机构，它面向的是各关键基础设施部门，不论是政府还是工业界的安全问题，以保障这些部门的关键基础设施。

## 2. 背景

保护关键基础设施的安全、组织国家级的信息保障工作的愿望缘起于1997年成立的“总统关键基础设施保护委员会”。2002年10月发布的第13231号行政令《信息时代的关键基础设施保护》又对该委员会做了改编。上述工作思路需要为每个关键基础设施部门都确定一个相应的联邦专门机构，作为该部门中信息保障行动的发起机关，还要为每个关键基础设施部门都指派一位部门协调员，与工业界密切合作，共同面对关键基础设施的挑战。

很多机构和个人参与了这篇战略纲要中的信息保障工作，对各自部门的安全战略做出了贡献。人们也意识到这种合作的意义。积极参与可视为一种正面的努力，但它只有通过不懈的合作和信息交换才能得以全面实现。所有的参与者都面临着大量的机会，这种机会不但落实在各部门自己的工作中，还表现在跨部门的合作以及公共-私营合作联盟之中。我们在此向很多机构和个人致以谢意，是他们促成了本篇纲要以及各个部门级的安全战略的出台。这是一种信号，反映了在保护信息系统和关键基础设施的过程中各方的不懈投入与合作。

## 3. 介绍

本节的重点是各关键基础设施部门所共同面对和关心的6个共同问题。基础设施工业的所有者和运营者意识到，关键基础设施保障不只是一个国家的安全问题，还表现为地区性以及全球性问题。人们对技术的应用不断增强，包括 Internet、实施生产和交付系统等技术，这一趋势制造了复杂的互依赖性，影响到了美国的地区、国家以及全球利益。我们正在日益变得互联，

正越来越依赖于信息系统。这种互联性催生了对高度的经济安全和可信的电子商务的需求。这一过程的核心在于公共-私营合作联盟，在于一种新型的合作结构，以协调商业界和政府在国内外的信息安全行动。当我们的全球性信息互联正在不断提高我们的生产力、促进我们的成长时，新的脆弱性和可能的破坏事件，甚至是攻击也随之而来。

虽然很多问题都在多个基础设施部门中存在，但不同部门间的情况也有很大不同。例如，某些部门已经建立了协调和信息共享机制，涵盖了其大部分甚至是全部机构和成员，以此来促进部门级的事件响应。而有的部门还正处在建立这些机制的过程之中。各个基础设施部门在制定其部门级安全战略中取得的进展各不相同。有的战略包含了行动的目标、行动列表以及进度；而有的部门只不过在战略中给出了一个大纲，向其成员略作鼓励而已。因此，这些战略在细节和深度上有所差异。

- 互依赖性：各基础设施部门的运营彼此互为依赖，互联性越来越紧密。
- 研究和开发：工业界和政府需要制定出研发规划，确定出新的研究领域，促进研发工作的进展，向研发工作追加新的投资。
- 教育和人才发展：意识培养和教育始终是一个大问题，即使是在“9·11”事件之后。
- 信息共享：所有的基础设施部门要确定出其对于不同部门间以及公共-私营之间的信息交换需求。
- 公共政策和法律/法规问题：信息自由法（FOIA）、反托拉斯法以及责任法都会对公共-私营合作造成阻碍。
- 国际问题：基础设施的运营超出了美国的物理边界，要面对很多不同的国际问题。

#### 4. 各部门面对的共同问题

##### （1）问题一：互依赖性

基础设施的互依赖性指关键基础设施之内以及各关键基础设施之间存在的物理的、电子的、经济的（电子商务）联系。除了这些基础设施之间的依赖关系外，它们还要依赖于地方、州以及联邦政府的支持，确保在危机事件中能够保持充分的预警、保护以及重建功能。这些关系中最容易确定的是各部门间的运行依赖性。然而，不太容易确定的则是，基础设施间在不同程度上还存在着间接的、千丝万缕的其他关系。互联性的增强带来了关键基础设施之间互依赖性的增长，这种互依赖性则进一步加剧了基础设施面临的风险，一旦某一基础设施发生故障，其他基础设施也会受到牵连。

工业发展面对的是一个基于信息社会的大市场，不论是从物理还是业务的角度来说，各机构的运营战略必须做出调整。目前已经做出的战略调整便直接来自对电子技术的应用及依赖性，这反映出各机构在迅速扩张的市场中的生存需要，意味着新的战略联盟的形成以及电子商务的应用。传统的业务和控制系统都是为封闭、可信的环境设计的。然而，当这些公司参与到信息社会之中，引入了新型的合作与交易关系时，它们的风险随之加剧，对大量其他系统的互联有可能使其遭到毁灭性打击。

于是，除了各机构要极大地依赖运营所需的专业技术和流程外，信息技术（IT）的日益采用也制造了关键基础设施之间的技术互依赖性，对信息空间的风险起到了放大作用。然而，我们已无法再回到过去，电子商务的迅速出现已经影响了很多企业结构的重组，使很多基础设施

发生了物理的变化，这些都已无法倒退。因此工业界必须马上实施信息保障战略，对其已经向IT投入的资金加以保护。

#### （2）问题二：研究和开发

关键基础设施保护中的研发需求是以往的传统性研发模式所无法满足的。这些新的研发需求涉及的内容包括物理及电子信息安全，以及由于关键基础设施中不断增长的复杂的互依赖性所带来的崭新的威胁和脆弱性。由于政府各机构的研发基金都受其预算的约束，私营工业在开展自己的研发活动时很少去考虑公共部门的有关工作，因而当前美国的研发工作非常支离破碎和缺乏协调。

完全依靠自然市场的推动力无法对基础研究给予足够的投入。而且，成本竞争以及法律法规的不确定性常使得各公司不愿向安全投资。这些挑战呼唤新的研发框架的出现，需要开展公共-私营研发合作，减少重复性研发，优化整个安全界内的研发活动。在这种框架内，研发需求将得到重新的审视、研发资源将得到更新和加强，安全模型中的不足也会在其中得到标识和关注。为了取得成功，需要结成一种前所未有的合作联盟，组合政府、学术界、私营工业中的最优秀的资源。

研究活动的范围包括三个领域：技术性研发活动，以发明新的关键基础设施保护技术；制定脆弱性评估的安全标准；开发工业界中最佳的操作规范，包括应急计划。上述三项工作面临的关键约束是缺少及时、准确的脆弱性信息。于是，除了对当前研发中的不足做分析外，研发计划中还必须对各关键基础设施的运营进行评估和分析。评估和分析后的结果应该在政府和工业界中共享，以定义出关键基础设施保障的研发优先级。在优先级得以确定后，研发路线将要为其提供一种全面的基石，以建立政策和战略，展开研发行动。PCIS 已经启动了研发路线的制定工作，但仍需要有范围更广的工作，覆盖全面的基础设施保护需求，包括物理保护、新政策以及协调机制。

#### （3）问题三：教育和人才发展

在面对攻击时，一个机构内最有价值的防御力量在于其人员，即要有理解并支持安全策略和流程的雇员和管理层。安全问题的解决所需要的是多种级别的理解力：所有的系统用户都应意识到可能的安全事故；他们必须在其本职工作上担负起相应的责任，对攻击做出必要的预防；他们必须知道，当攻击真正发生时应该如何去做。通过安全意识的培养项目，要能够使用户掌握安全工具的正确使用方法，知道如何实施安全控制，由此创建一个安全的体系结构环境。雇员将从中学到应采取哪些行动来减少基础设施遇到的综合风险并缓解安全事件的危害程度。而且，坚持不懈的推广工作可以使所有雇员的头脑中始终铭记安全操作规范，使他们共同参与到对安全问题的解决行动中来。学习安全知识，加强专业水平，发扬创造力，这将使可用的安全资源得到很好的扩展。

#### （4）问题四：信息共享

很多危险或非法集团，如黑客、毒品贩、有组织犯罪集团或恐怖分子等，经常互相交换他们发现的系统脆弱性以及用来攻击这些脆弱性的工具。而与此对照的是，市场经济中的企业，往往出于竞争的原因，不愿意在彼此间共享安全信息，这对他们非常不利。现在，面对着层出不穷的威胁和脆弱性，工业界和政府需要通力合作，从而促进信息流的协调。

到目前为止，互为依赖的各个关键基础设施部门之间已经建立和发展了很多协作框架，以便于共享安全信息，如威胁信息、脆弱性信息、对策或最佳操作规范。在这些已有的协调机制

下，有些机构已成立了信息共享系统，而有此机构还需要继续在这方面做新的工作。除了促进部门级的信息共享外，有若干基础设施部门还开始筹建超出单个工业界范畴的信息共享机制，如与多个部门或政府实现共享。

#### （5）问题五：公共政策和法律/法规问题

虽然各个私营部门之间已经开始在共享安全信息，但与政府的类似信息交换却非常复杂。目前，有三项法律为信息保障中的公共-私营合作造成了障碍：信息自由法（FOIA）、反托拉斯法、责任法。

在 FOIA 的要求下，美国政府行政部门持有的记录应该向公众公开。虽然，美国国会认识到了某些信息有着不可披露的合理需要以及通过法规、条例来促进合作的现实需求，并因此而规定了信息披露的豁免情况，然而，当前 FOIA 中规定的所有豁免情况是否能够对披露中的威胁和脆弱性信息提供足够的保护，这还有待于私营工业的确认。人们关心的是，出于关键基础设施安全意识培养以及安全规划的目的而资源共享的信息，有可能会应 FOIA 的要求而披露，而站在披露请求另一面的，可能是竞争者、诉讼者，甚至可能是居心叵测的攻击者。

此外，对于如何实施 FOIA，很多州和联邦机构都有不同的规则。这造成了不同的基础设施部门以其自己的方式看待 FOIA。为以防万一，它们不愿意同地方、州和联邦政府共享安全信息，除非 FOIA 中的模棱两可得到了彻底的澄清。在州政府级别，这一问题更加严重。

反托拉斯法也为信息共享添加了障碍。合法的商贸业务及其关键信息的交换行为应该不受联邦和州政府反托拉斯法的禁止。不论其出发点如何，工业企业之间的某些协约、合作协定以及信息共享有可能成为反托拉斯的对象，如提升价格、削减产出等。ISAC 的目标是清晰的，然而，市场中一些企业发生的类似简单合作却有可能被其他未参与合作的公司、机构以及其他非政府组织所怀疑，于是，ISAC 的成员不得不面对反托拉斯的风险。

最后，信息安全的专业公司以及某些 ISAC 不愿意制定安全标准。因为当这些标准出现问题时，它们将被迫陷入责任法诉讼。

#### （6）问题六：国际问题

某些关键业务部门已经建立了强有力的覆盖整个北美的跨边界基础设施联络关系。然而，由于基础设施的很多无缝连接，大多数机构都认为基础设施保障应该是一个全球问题，如 Internet 便没有边界。在同样的一条国际通路中，有益和有害的信息流通常夹杂在一起高速运行。而且，美国的基础设施还要依赖于很多外资的关键机构，其中还有很多特殊的安全问题。脱离于对国际经济影响的考虑而处理美国的国家安全问题是不全面的，而且也难以奏效。

大多数国家已经在国家基础设施保护战略的工作中达到了成熟阶段，与这些国家的工作相融合，并在可能的地方对他们产生影响，有利于全球经济发展，避免留下国家基础设施保护孤岛。这些国家的基础设施保护项目应该合作，表现为一个集成的方法学，使全球的基础设施系统能够联合工作和运行。

然而，在跨越国界的合作中，社会、文化、政治准则是不能忽视的。如果不能适应不同文化对安全、隐私以及政府或工业控制的不同理解，便会不可避免地导致国际合作中的冲突和矛盾。例如，很多国家仍然需要对关键业务部门实现私有化，它们对安全保障和信息共享的看法可能与美国的公共-私营合作联盟所持有的观点大不相同。

最后，与 IT 伴随而来的风险直至现在尚未得到全面认识，合并、采办以及联盟（和分拆）均涉及现有网络的连接和/或集成（或者隔离）。在某些国家中，信息资产中可能还要包括与海

外或国外市场的连接，这些系统或其所含信息遭到的任何破坏均会导致严重的后果。因此，必须投入大量的努力，保障这些日益国际化的基础设施的完整性。

## 5. 总结

本篇纲要代表了工业界的观点，表现了各工业部门已经采取的关键基础设施保障行动。“9·11”事件突出了跨工业部门合作的重要意义，强化了继续推行合作的迫切需求。工业界保护其关键资产的决心正在不断增强，这是对信息和物理威胁、脆弱性及安全事件的响应，以期当进入一个不断变化的后“9·11”环境时，我们能够顺利实现遏制、预防、减缓、响应、重建以及学习等工作。“9·11”事件提高了美国人民的意识，阐明了国家反恐活动的需要，但工业界的关键基础设施保障工作并不是一个新话题。本文提出的讨论和建议不是这9个月以来工作成果，而是代表了工业界多年来履行的关键基础设施保护以及整个工业界内的信息保障协作与对话。

本篇纲要包括了来自很多关键基础设施部门的贡献。它们意识到，关键基础设施保障工作离不开复杂的战略，没有持续的公共-私营合作联盟，任何单一机构都无法有效地解决基础设施保障问题。然而，很多问题仍然存在，经过通力合作，政府和私营部门可以实现我们的共同目标，保护好我们的关键基础设施，使之不受信息和物理攻击。



---

## 九、研发项目开发计划：通过信息安全技术 实现关键基础设施保护（摘要）

关键基础设施保护合作组织（PCIS）

2002 年 2 月

---



扫二维码阅读全文

## 1. 介绍

### 关键基础设施研发项目计划

所谓关键基础设施保护（CIP），涉及运用信息安全（InfoSec）技术和方法抵御来自网络对支持或影响关键基础设施（CI）运行的 IT 系统的攻击。如今，我们的社会存在着远还没有化解的巨大风险，尤其是恐怖主义攻击的风险，其中包括针对既定基础设施目标的协调一致的网络攻击。这些风险之所以高悬我们头顶始终阴魂不散，是因为对适用于关键基础设施信息技术系统的信息安全手段。我们在其有效性和实用性方面还缺乏应有认识。我们所了解的只是以下两个最突出的问题：

- （1）关键基础设施的信息安全技术需要在多方面得到改进。
- （2）这些方面包括一些已知不足和很多未知不足。这些不足的存在是由于我们对以下两点情况缺乏了解而造成的：

- 关键基础设施信息技术现存的脆弱性；
- 用以消除脆弱性（尤其是在网络恐怖主义日益猖獗的情况下）的现有信息安全技术的有效性和实用性。

由此可见，就制定一项“关键基础设施保护信息安全研发项目开发计划”而言，我们还缺乏大量的必要信息。这样的“关键基础设施保护信息安全研发项目计划”对于指导和实施作为关键基础设施保护国家战略组成部分的关键基础设施保护研发工作来说，具有不可估量的价值。如果没有这种计划，有价值的研发工作也肯定会开展起来，但是我们不会更明智地对待由研发工作提出的最关键性的信息安全需要是否得到满足的迫切问题。

然而，我们可以通过大量工作来接近这样的项目计划，这些工作在第 3 章“项目开发计划”中得到描述，该计划中要详细阐明制定“关键基础设施保护研发项目计划”需要做哪些工作。本文便是这种“项目开发计划”的一个草案，它是关键基础设施安全合作组织（以下简称“合作组织”）（PCIS）主持的一项研究的成果。

### 合作组织的任务和研发工作的作用

合作组织致力于联合工业界<sup>①</sup>和政府部门<sup>②</sup>，“提高和确保关键基础设施服务<sup>③</sup>的可靠供应，以应对经济和国家安全所面临的不断涌现的风险。”<sup>④</sup>应第 1 版《信息系统保护国家计划》（以下简称“第 1 版国家计划”）的要求，关键基础设施安全合作组织于 2000 年 2 月成立。合作组织的任务是“协调跨部门方案和补充公共-私营部门做出的努力，提高并确保关键基础设施服务的可靠供应，以应对经济和国家安全所面临的不断涌现的风险。”<sup>⑤</sup>

合作组织下设若干工作组，研发工作组便是其中之一。该工作组的任务是努力制定出一个

---

① 成员有 70 多家私营公司和 13 个政府部门，参见附录所列董事会成员名单。

② 关键基础设施安全合作组织应“国家计划第 1 版”第 8 项第 8.1 节第 4 款重要事件 8.2 的要求创建。

③ PDD-63（5/22/98）定义的关键基础设施（CI）包括能源、金融服务（FS）、运输、通信和信息服务（C&IS）、重要民生服务[其中包括医疗保健、安全和供水（VHS）]。

④ 关键基础设施安全合作组织观点的陈述，详见 [www.pcis-forum.org](http://www.pcis-forum.org)。

⑤ 参见“国家计划第 1 版”第 8 项第 8.1 节第 4 款重要事件 8.2（重点为 73~116 页）。

研发项目开发计划来。这个计划堪称一幅“近期研发布局图”，上面标明的活动包括了用以引导当前信息安全研发朝着满足关键基础设施保护需要的方向发展的差距分析，同时还涉及了制定项目计划所必需的多项相关准备。本文描述了这些工作。不仅“研发布局图”所列开发工作的成果，就连开发过程本身都是为了给网络空间安全研发工作奠定一个强大、灵活和综合性的基础。这个基础是相关政策、评价、战略和行动的基石，可以大幅度改善关键基础设施的安全状况，从而保持相互依存的关键基础设施部门的稳定和持续运转。合作组织的研发工作是所涉范围更广的关键基础设施保护框架性文件“信息系统安全国家战略”<sup>①</sup>（目前正在制定中）的准备工作的组成部分。

### 范围和现状

制定本工作草案的目的是为筹划一项用以支持信息技术系统关键基础设施保护的研发项目开发计划（这是合作组织任务的重要组成部分）做基本准备。这种准备工作包括（但不限于）一份完整的定义、假设和目标清单，可补充和支持合作组织对国家战略的贡献。本文是有关定义的工作草案，是在合作组织第四工作组<sup>②</sup>指导下完成的，它将构成第四工作组对合作组织所提建议的内容。

因此，本项目开发计划的目标是完成两项工作。第一，它将在高层定义用以支持信息技术系统保护的研发项目的开发所需完成的任务，同时将概述最终定义研发项目的基本原理和方法，研发项目中包括可能由合作组织和 / 或关键基础设施保障办公室（CIAO）发起的试验性活动。第二，它将支持合作组织应总统令（PDD63）的要求就制定“第 2.0 版信息系统保护国家战略”（以下简称“国家战略”）提出的研发建议。

本工作草案的范围是记述研发项目预计的已知要素、定义未知或未被充分认识的要素，并描述必须把所有要素包含在内的各项任务。这些以开发研发项目为目的的任务，是以表现一组相关关系的方式描述出来的。换言之，研发项目的相关图可以为如何达成研发项目开发计划提供一个定义结构。列出这些任务，意在构成一个记述完整的综合性高层计划（基本原理和方法也包括在计划内），用以指导合作组织以及其他任何从事通过信息安全技术实现关键基础设施保护研发工作的辅助性组织的研发活动。此外，本文还概述了将在合作组织领导下实施的试验性研发活动，以接近于制定出一个全面的关键基础设施保护研发项目开发计划。

这个项目开发计划的最终草案，旨在成为一份综合性的文献，容纳了很多关键组织提供的输入。这些组织参与或监督了各项研发工作或即将参与或监督研发计划的未来版本中定义的任何其他任务。然而，这个“最终”草案还要成为一份“活”文件，将描述运用必要信息达到制定研发项目开发计划目标的进展情况。而该研发项目开发计划将用来指导和追踪以关键基础设施保护为对象的信息安全研发工作。

### 本文概述

本文第 2 章“现状分析”对关键基础设施保护、基本威胁以及对关键基础设施保护研发项目各个方面都产生了推动作用的紧迫挑战进行了现状分析。第 3 章“研发项目开发计划”是本文的核心部分，介绍了开发关键基础设施研发项目的计划。项目开发计划在很大程度上依赖于

<sup>①</sup> 详见 [http://www.ciao.gov/CIAO\\_Document\\_Library/national\\_plan%20\\_final.pdf](http://www.ciao.gov/CIAO_Document_Library/national_plan%20_final.pdf)。

<sup>②</sup> 关于关键基础设施安全合作组织其他工作组的情况，请参阅附录。

多项近期任务、后续任务、各项任务的互依赖性、各项任务的完成结果以及执行中的关键基础设施保护研发项目的目标。第4章“CIP中的InfoSec技术研究领域”详细描述了技术研发的若干方面。第5章“CIP中的InfoSec运行研究领域”对实施研究任务进行了详细的补充说明。第6章“总结”归纳了研发项目计划以及本文推荐的后续步骤的基本原理。

## 2. 现状分析

在概述研发项目关联性以及制定项目计划的各项任务之前，本章将首先对导致本文之所以做出这些研发方法建议的当前现状做一番阐述。当前的状况称得上是我们所面临的一大紧迫挑战，其中包括未被充分认识的信息安全脆弱性、运行和技术方面的困难以及旨在保护关键基础设施的研发项目的缺乏。

### 基本网络威胁

基本网络威胁，是指任何人有可能在任何地点利用互联网或其他公共、专用网络，未经授权进入关键基础设施资产的运营机构的IT系统。这些关键基础设施的运营者，往往是那些试图未经授权进入系统的敌对分子的首选目标，他们的目的无非是恶意修改运营者的IT系统，从而阻止基础设施提供服务或泄露相关涉密信息。我们国家面临的最大的网络恐怖主义威胁是国土攻击，网络破坏者、黑客、窃贼、“电脑迷”以及其他形形色色在各种系统上寻找信息安全脆弱性的人的小打小闹绝对无法与这种威胁同日而语。

最应引起我们警觉的情况是，敌对分子像在“9·11”事件中那样，丧心病狂地对物理设施和虚拟网络同时发起攻击，这种情况最有可能在地区、全国乃至国际范围内造成多重的、同时的、连锁性的破坏。有了“9·11”事件的先例，我们已经不难想象，恐怖主义分子一旦对空中运输控制雷达计算机和网络发起攻击，使雷达系统追踪偏航飞机的能力降低，进而使空中其他飞机面临的危险大大增加，将会是怎样一幅物景。其他有关的危险情况，还包括敌对分子对供水控制系统同时进行网络 and 生化武器攻击。对供水控制系统的这类攻击，可能会使社会公众在不知不觉中受到化学或生物制剂的伤害。

这类威胁的对象，绝不仅仅限于关键基础设施运营者的IT系统，凡是由于设计缺陷、疏忽大意或者对信息安全的脆弱性不了解或不重视而可以任人随意通过互联网进入的系统，都面临着这样的威胁。互联网只是一个攻击媒介而已，一次成功的攻击无论借助何种媒介，暴露出缺陷的系统都有可能被用作下一次攻击的登录点。这种连锁攻击，最终会导致恶意滥用IT系统的情况出现，从而使攻击者得以控制或直接影响对基础设施提供服务的至关重要的系统。

其他攻击媒介，还包括某一关键基础设施运营者的IT系统与其伙伴组织（其中从作为合作伙伴的同一公司的业务部门到其他关键基础设施运营者，涉及的范围很广）的IT系统之间的专用网络连接（真实连接或VPN连接）。合法进入此类附属系统的人（如附属机构雇员之类的内部人员），或者能够得到授权进入系统的外部人员，都有可能滥用访问权，从而对关键基础设施运营者的目标系统形成攻击。最近的恐怖主义活动明显表明，蓄意作恶的敌对分子将千方百计并且有能力取得内部人员资格，以获得访问权或相关信息，进而把这种内部人员资格转变为一种攻击能力。

由这种“连锁攻击”造成的基本网络威胁，是各国关键基础设施运营者高度相互依赖的必

然结果。相互依赖问题将在后面进一步讨论。

### 紧迫挑战

由于存在这样的基本威胁，我们面临以下四种紧迫挑战，它们不仅会影响行之有效的研发项目的开发任务，同时还会对改善关键基础设施运营者网络安全状况的近期任务产生影响，从而使运营者由于其信息系统缺乏相关设计而无法应对新的网络恐怖主义威胁。

### 未知的脆弱性程度

基本网络威胁尤其应该引起我们的警觉，因为当今存在着另外一种紧迫挑战，即我们会遭受攻击的关键基础设施运营者的 IT 系统的脆弱性缺乏充分认识。除了银行与金融部门的某些环节存在明显例外以外，关键基础设施普遍没有积极投身到商业信息安全实践中来，没有运用现有信息安全技术和流程进行脆弱性评估。事实的确如此，直到最近，也仍然有很多关键基础设施运营者不把自己的 IT 系统视为高风险、高价值资产，并没有认识到他们应该受到额外的妥善保护。同样，对于评价信息安全的脆弱性，人们也普遍缺乏积极性。

因此可以说，对于我们国家的关键基础设施信息系统面对网络恐怖主义究竟有多脆弱，我们实在是知之甚少。同样，对于现有信息安全技术究竟在多大程度上应用到了关键基础设施保护之中，这些应用产生了多大效果，信息安全技术在关键基础设施 IT 系统中的应用还存在多大差距等问题，我们也是不甚了了。同样的情况还包括用于使用和管理信息安全技术的通用信息安全处理方法，以及旨在保护技术安全机制（如物理和人员安全）的对非技术安全手段的应用和管理。

然而，如果我们对关键基础设施系统的脆弱性缺乏具体的、准确的和全面的了解，我们就很难搞清应该如何运用信息安全技术来降低近期风险，同时也很难搞清应该如何通过信息安全技术开发来提供具有长期效果的更好的保护方式。下面列出的部分问题表明了这方面问题所涉及的范围：

- 我们应该如何通过更好地运用现有信息安全技术来根除脆弱性，以使我们的关键基础设施系统更有力地抵御当今的攻击？
- 我们应该如何通过定义“标准”手段或“通用实践措施”来使现有信息安全技术应用到关键基础设施之中？
- 当今的信息安全技术在现存脆弱性方面以及在面对威胁时（尤其是面对针对关键基础设施或部门的威胁时）具有哪些局限性？
- 我们需要在哪些方面开展技术研发工作以真正缩小差距？
- 我们需要开发哪些新的通用处理方法来管理这些差距带来的风险并为应用不断涌现的新信息安全技术做好准备？

由于缺乏对这类问题的答案，我们只能通过筹划两种行动来扩大我们的信息库，从而得以真正了解和控制国家关键基础设施系统所面临的风险。

首先，从中期和长期角度而言，我们期望关键基础设施运营者不断加强信息安全的脆弱性和风险评估工作，同时主动应用信息安全技术，开发出能够满足关键基础设施运营者和部门最迫切需要的通用处理方法。这些努力应与关键基础设施部门内和部门间加强信息共享、解决 FOIA 放宽公共-私营部门之间信息共享之类政策问题、鼓励开展预算外信息安全活动、鼓励部门内和部门间合作实施新的信息安全方案等其他方面的工作从根本上结合到一起。

其次，我们需要通过近期行动，来加强对我国关键基础设施 IT 安全现状的了解。虽然，需要长期付出巨大努力，才能对国家关键基础设施的脆弱性做出恰如其分的评估，但是，新近开展的研发项目，能够而且应该包含涉及关键基础设施系统的 IT 应用的运营研究。试验性运营研究可以从阐明上述问题开始（事实上，这方面的试验性研究已经帮助我们懂得了应该如何阐明上述问题），继而将研究成果应用到当前正在运营的具有代表性的现实世界系统之中，最终确定应该用哪些现有信息安全技术和处理方法来消除现存的脆弱性。

### 复杂性

当前的脆弱性评估和正在进行中的研发项目，都因关键基础设施的错综复杂而困难重重，而这些复杂性构成了更为紧迫的挑战。各个系统之间的相互依赖（这个问题将在下文中讨论）会扩大一次攻击的潜在影响范围，因为对某一关键基础设施系统的攻击能否取得成功，可能取决于其他关键基础设施系统。只有这样，攻击的影响才有可能在多个系统内繁衍蔓延。连锁影响和连锁攻击之所以令人忧虑，不仅因为各个系统相互依赖，而且因为网络的融合已经成为一种程度越来越高的发展趋势。其中，从数据 / 电话网的融合，到多公司共享的电子事务处理，再到关键基础设施服务提供商的网络和计算机与其他关键基础设施服务提供商的网络和计算机的共同运行，凡此种种，不一而足。在如此形成的新威胁环境中，对多重信息领域的持续性影响，极有可能使传统上被视为多余并容忍错误存在的信息源遭到各种不法行为的破坏。

除了广义的复杂性之外，我们还要面对更为具体的技术复杂性，它们产生于现行通用处理基础设施（即现有信息安全技术的运行对象）与用在关键基础设施 IT 系统中的各种专业系统之间的矛盾。其中，最为关键的是嵌入关键基础设施运行心脏的控制系统，即广泛用在从制造业到发电厂的各个部门的不可或缺的系统，我们的关键基础设施系统离开了它们就无法运转。这些控制系统因其对关键基础设施服务的直接控制，构成了最重要的资产。大多数控制系统和网络在技术上存在着巨大的差异，而它们设计的现行信息安全技术也必然会千差万别。当前，适用于这些控制系统的信息安全技术十分缺乏，抑或说，无论在基本保护还是在充满网络恐怖主义威胁的新环境方面，对于哪些技术适用于这些控制系统、哪些技术不宜用于控制系统，我们实在知之甚少，这是一个应引起我们高度警觉的问题。很多技术差距和研发差距之所以存在，可能就是各种各样专业系统与比较常规的计算系统之间的复杂交互作用造成的。

即便撇开关键基础设施控制系统的安全问题不谈，也存在着复杂的信息安全挑战。它们是典型商业处理方法与关键基础设施运营者之间在信息技术上相互依赖的综合作用结果（后文将对此做详细讨论）。

### 研发协调、信息共享和合作

关键基础设施和网络安全是涉及范围极广的问题，任何行业都不可能独立将其解决。这种挑战绝不是传统的政府主持的研发形式、私人出资的研发形式和大学的研究形式所能应付得了的。然而，当前的信息安全研发工作却处于一种支离破碎、毫无调度的紊乱状态——众多政府拨款部门各自按照不同的计划行事，而私营研发工作则几乎从不考虑政府研发工作的布局。政府多个部门之间的信息安全研发投资、由政府实施的信息安全研发、几乎互不关联的公司出资和实施的信息安全研发造成了混乱，从而为信息共享、研究协调和设定研发的优先级带来了极大的挑战。

因此可以说，在当前情况下，对实施中的各种形式的研发工作进行全面和准确的归类是不

可行的，然而这种归类却是以下几项活动的先决条件：评估与关键基础设施相关的信息需求、确定正在进行中的关键基础设施研发项目的工作重点，以及确定各行业的信息安全研究工作进行新合作和潜在协作的新前景。以下这些活动是弥补现行研发工作以下缺陷所必不可少的。

- 信息安全研发可能没有与关键基础设施直接相关。大多数传统信息安全研究都是仅仅基于 TCP / IP 网络以及标准商业操作系统和软件开展的。由于控制系统并没有完全分享这种技术基础，因此现行信息安全具体而言可能与操作系统无关，总体而言可能与关键基础设施和网络无关。
- 当前的研发都是出于商业用途开展的。当前的研发对象是可在商业界通用的技术和方法，以及可供军方/政府用于各种用途的相同的 COTS 技术。
- 当前的研发是以单一所有者/运营者模式开展的。当前的信息安全技术都是以单一所有者/运营者模式开发出来的。在实际工作中，相互依赖的关键基础设施系统具有很高的相互关联性，因此难免产生涉及多个运营者系统的信息问题。虽然，这样的情况在一定程度上存在于比较典型的商业处理中，但是人们往往并不将其当作技术问题来处理，而仅仅认为它们属于商业问题的范畴。然而在关键基础设施处理中，一个系统由于另一个系统的原因遭到破坏的风险却是根本不可接受的风险。尽管有限的少数涉及企业外联网和电子商务的“跨企业安全”研究把重点放在了有控制地扩大安全范围上，但是当前的信息安全研发工作都不是以开发解决这些相互依赖问题的方法为目的的。

#### 关键基础设施部门的协调和信息共享

要想评估当前的脆弱性、制定标准、定义差距和研发需要，各关键基础设施部门就必须通力合作。这种前所未有的信息共享和合作，应该涉及共享各关键基础设施运营者的脆弱性评估信息、比较各种通用矫正手段、开发可满足部门信息安全需要的通用方法、确定方法或技术上存在的差距。这些合作，对于适宜保护我们的基础设施网免受网络攻击乃至预防会造成连锁破坏的意外事件来说，也是必不可少的。

这样的合作其实已经开始。其中，以信息共享和分析中心在若干关键基础设施部门做出的努力效果最为显著。在各个部门内共享现有信息的努力，会为从工业界到政府部门的整个关键基础设施业内更广泛的信息共享和合作打下坚实的基础，进而可以提高和共享对技术或方法脆弱性和差距的认识。

然而，主要侧重于信息共享和分析中心的合作（这是至为关键的最初步骤）远不足以形成一个探讨关键基础设施信息安全脆弱性评估及相关问题的论坛。此外，了解脆弱性与关键基础设施防范网络攻击，往往是同时并进的。当前，预防灾害的责任呈高度分散之势，各部门形成了各自为战的局面：地方政府和州政府在某些联邦部门的参与下，负责确定以何种方法应对会使某个关键基础设施运营者的服务质量降低乃至瘫痪的攻击或意外事件；而关键基础设施运营者则负责消除攻击或意外事件造成的内部影响。因此，信息安全方面的协调合作还涉及针对灾害预防的协调合作。

#### 互依赖性

所有这些紧迫挑战，被关键基础设施运营者之间的高度互依赖性组合到了一起。互依赖问题涉及物理运行（关键基础设施服务的提供）、信息共享以及保护和响应技术等诸多方面。而在互依赖性的每个方面都存在着越来越恶化的若干因素，使研发的问题显得日渐突出，原因就

在于关键基础设施业界人士对现有的安全技术和信息安全研发工作缺乏足够的重视。

我们的关键基础设施，不仅在运行上相互依赖，而且这种依赖性正愈演愈烈。每个部门内部的关键基础设施的运营，都越来越依赖于相关的信息技术，同时通过专用网络和公共互联网相互联得越来越紧密。由于存在着如此广泛的相互关联，我们的关键基础设施正面临着巨大的潜在破坏。这样的破坏会在局部、国家乃至国际层面上造成多重的、并发的和连锁性的破坏。<sup>①</sup>

有了“9·11”事件的先例，我们已经不难想象，恐怖主义分子一旦对空中运输控制雷达计算机和网络发起攻击，使雷达系统追踪偏航飞机的能力降低，进而使空中其他飞机面临的危险大大增加，将会是怎样一幅场景。其他相关联的危险情况，还包括敌对分子对供水控制系统同时进行网络和生化武器攻击。对供水控制系统的这类攻击可能会使社会公众在不知不觉中受到化学或生物制剂的伤害。

### 运行性互依赖性和网络互依赖性

互依赖性有两种基本类型。第一种，每个基础设施公司都需要其他部门提供的基础设施服务。因此，一个部门出问题会对其他基础设施部门产生连锁影响。例如，供水公司依赖交通部门运送化学制剂，如果后者因遭受攻击而无法正常运转，就会造成前者供水短缺、服务质量下降和风险增大。

第二种互依赖性是由这样的情况造成的：很多基础设施公司的计算机系统要定期与其他公司的处理系统发生联系，结果每个关键基础设施运营者的处理系统都要依赖其他公司的处理系统（其中包括其他基础设施服务提供商以及供应链上的其他公司和合作伙伴）。

由于IT系统日趋复杂，第二种网络方面的互依赖性大幅度增加了关键基础设施IT系统所面临的风险。例如，多网络接口中，会为关键基础设施网络攻击提供多个进入点，而对某个公司系统的每次网络攻击，都会有机会对其他公司的系统发起连锁攻击。网络方面的互依赖性对技术和研究方案提出了不可忽视的要求：这些方案必须能够解决由于所有者、运营者、部门和相关技术之间相互依赖而给关键基础设施带来威胁的问题。

### 连锁破坏和连锁攻击

互依赖性有可能产生两种连锁性结果：间接破坏和间接攻击。连锁性间接破坏产生于运营或后勤保障上的相互依赖，这使得关键基础设施在攻击面前总体上显得十分脆弱。例如，（由电子攻击造成的）运输服务瘫痪，会使运送供水系统用于水处理的化学制剂的工作无法正常运行，从而造成化学制剂储备下降乃至无法正常供水。

连锁性的电子攻击，是从各关键基础设施运营者之间的网络连接点上着手进行的。例如，某运输服务提供商遭到一个网络攻击者入侵，后者随后可以利用该运输服务提供商与某个供水服务提供商之间的网络联系，直接进入供水服务提供商的控制系统，从而让供水工作陷于瘫痪。因此，该供水服务提供商的安全取决于该运输服务提供商的安全，然而运输服务提供商的系统安全并不在供水服务提供商的控制之下。

信息安全研发工作必须强调电子依赖性，以及用以化解连锁性电子攻击风险的手段。后勤保障的相互依赖是运营研究所必须重点考虑的问题，这方面的工作应该开发出适宜的模式，用

---

① 多重破坏和连锁破坏的例子待定。它们有两种类型：连锁性电子破坏（从电子形式到电子形式等）和连锁性间接破坏（从电子形式到物理形式再到物理形式等）。



以推动相关各方共同做出努力，化解连锁性间接破坏的风险。

关键基础设施运营者不仅依赖其他关键基础设施运营者，同时还依赖与其有业务往来的其他公司（例如，关键基础设施运营者会与其提供商共同使用某一自动供应链管理设施），这就使网络依赖性的问题变得更加复杂。这样的情况要求在企业之间建立安全机制。但是，在企业间目前的基本安全状况下，很难确定是否存在涉及关键基础设施的安全要求。也就是说，在两种网络依赖性（即基础设施内的电子联系和关键基础设施运营者 / 提供商之间的电子联系）间可能存在着重大差别。

关键基础设施的这两种依赖性，在所需要的保护、现有安全技术和满足这些需要的处理方法等诸方面均有很大的不同。以通常方式运用安全技术和使用典型的自动电子事务的处理方法，或许能够解决基础设施运营者 / 提供商的安全问题，但也有可能毫无作用。现有的信息安全技术，很可能并不足以满足关键基础设施的需要，因为残余风险在某些典型的电子事务环境中是可以接受的，但是在基础设施机构中却不可容忍。更可能的是，在基础设施内部，电子连接的信息安全需要是现有的信息安全技术所无法满足的，因为这些连接与生俱来就是双向的，而这样的相互依赖在典型电子商务环境中根本不存在。针对基础设施内部网络连接的安全处理方法，必须明显区别于基础设施提供者内部网络连接的安全处理方法。在前者的环境中，必须由双方共同承担安全责任；而在后者的环境中，由基础设施公司独自承担网络连接的安全责任就可以了。

### 政府政策问题

目前，有很多政府政策问题限制了各部门的协调和信息共享，而最为明显的是，它们限制了各部门为加强对现有脆弱性以及研发需要的认识而付出的努力。FOIA 和反托拉斯问题制约了协调和信息共享，因此应成为当前立法和制定法规工作的重点。

最突出的政府政策问题，或许非向关键基础设施运营者拨款开展信息安全现状评估和改善工作莫属。例如，加利福尼亚州首席信息官办公室最近对该州所属公共事业运营者进行了一次调查，发现不但存在安全状态之薄弱的情况，而且他们还计划进一步增加并提高自动化信息系统的复杂性，这着实令人担忧。虽然重要的安全问题已经得到重视，但是用以解决这些问题的资金依然是一个始终没有得到解决的问题。私营关键基础设施运营者也面临着同样的问题，他们同时还缺少开展信息安全工作的委托授权（后一个问题比前一个问题更严重）。既然有大量潜在的信息安全工作需要由涉及各个行业和部门的关键基础设施运营者来开展，政策专家就应认识到，这方面的费用最终要由政府承担（如通过政府发行长期债券、课税扣除和按规定减免关键基础设施消费者的使用费用等方式）。但是，从目前来看，政府还没有采取任何行动为关键基础设施的信息安全颁发委托授权或提供资金。

有一个相关的政府政策问题产生于关键基础设施行业或部门的“合理实践措施”概念（sound practices）中。这种概念构成了关键基础设施信息安全活动的标准化基础，为关键基础设施运营者评估自己在信息安全方面付出了充分努力提供了一种通用度量尺度。没有这样的“标准”，关键基础设施运营者便会在评估脆弱性以及通过研发工作弥补和确认技术及处理方法的差距方面，面临巨大困难。但是，除资金和对现存脆弱性缺乏认识问题之外的很多政府政策问题，制约了“合理的实践措施”定义工作的开展。需要付出多大努力才能实现制定适宜标准和确保处理方法合理的目标？政府在阐明和实现这些目标的过程中应该担任何种角色？政府

在推动各界接受和应用“标准”和研发成果方面应该发挥什么作用？关键基础设施运营者对安全应该有什么认识？诸如此类的问题，使有关如何制定标准或定义“合理的事件措施”的政府政策问题变得更加突出。当前，有关这些问题的政策责任涉及了联邦政府和州政府的很多部门。

### 3. 研发项目开发计划：任务及其相关关系

研发项目开发计划是依据可以近期开始执行的一组任务制定出来的。图 9-1（原文中遗漏此图——译者注）所示便是这些任务、结果和提供给其他任务的前馈信息，以及结果与任务之间的相关关系。本章将对每项任务及其关系加以说明，而以后各章将对其中的部分任务做详细论述并阐明它们的基本原理。本篇项目开发计划如果能够在关键基础设施业界（其中包括但不限于关键基础设施运营者、合作组织以及其他伙伴组织和协会）得以实施，将会带来以下结果：一个关键基础设施信息安全研发项目、针对现存关键基础设施网络脆弱性的近期矫正措施指南、朝着关键基础设施信息安全准则和最佳实践措施方向发展的实质性进步。

#### 信息安全技术研究

图 9-1 中从左上方朝向右上方的流程即是从当前活动朝着研发工作取得成功，并为关键基础设施保护开发出极具实用价值的信息安全技术的方向发展的流程。如前文所述，这个活动流程目前还面临着很大的困难，这不仅因为我们对关键基础设施信息技术的脆弱性不甚了解，还因为我们对本应由信息安全技术研发工作满足的信息安全需要还远没有得到认识。但是即便如此，我们依然能够确定某些方面的研发工作，这些项目既是关键基础设施保护的需要，而且也是目前还没有有效开展（或者说没有为 CIP 而开展）的工作。

图 9-1 中的绿色框“已知的研发差距”表示了已知研发需求的诸多方面。在此有两条活动途径。第一条是根据当前对关键基础设施保护需求、技术差距和研究差距的了解来定义研发目标。本文第 4 章对有助于填补关键基础设施保护领域当前存在的技术差距的多方面研发工作进行了说明。活动的第二条途径与第一条大体相同，不同之处在于它所依据的是目前对关键基础设施信息安全需要的零星了解的比较，其中尤以控制系统的保护为重。合作组织即将开展的一项工作，是召集各方专家列举关键基础设施计算与标准企业计算中现行安全技术之间不相吻合的情况。<sup>①</sup>如图 9-1 中右上方的蓝色框所示，这两条途径都可以得到有关“近期新研发目标”的信息。

这些新近注入关键基础设施保护信息安全研发项目的研发目标，可以帮助我们为关键基础设施保护开发出全新的信息安全技术；如图 9-1 所示，右上方的橙色框与图中所有其他橙色框一样，代表的是关键基础设施保护研发工作所取得的经得起论证的成果。新信息安全技术同时也是第二类研发工作的结果。这些研发工作旨在解决必须得到明确定义的课题，用以具体弥补信息安全技术方面的差距（图 9-1 中用蓝色表示的“面向 CIP 研发差距的 CIP 研发目标”，以表明这一类 R&D 工作）。

#### 关键基础设施的运行研究

旨在弥补关键基础设施保护差距的研发目标应该是下述过程的结果：该过程始于对关键基

<sup>①</sup> 这是一个有关安全数字 / 电子过程控制系统的样板任务，是 PCIS 与 CIAO 共同完成的。

基础设施信息技术的脆弱性进行的运行研究（见图 9-1 中左上方的顶部黄色框）。正如本文第 5 章详细描述的那样，关键基础设施的运行研究共分三类。第一类研究是针对信息技术运行和关键基础设施运营者的潜在安全脆弱性进行的，其中包括（但不仅限于）控制系统和运营者进行的常规企业计算。第二类研究着重针对关键基础设施运营者之间在信息技术方面的互依赖性以及脆弱性和与连锁攻击相关的对抗手段。第三类研究注重关键基础设施运营者之间在非信息技术和运营方面的互依赖性以及脆弱性和与连锁攻击相关的对抗手段。

所有这三类运行研究都可以为针对关键基础设施保护的研发目标提供前馈信息。无论是 IT/InfoSec 还是 InfoSec/互依赖性的运行研究，都能提供有关明显表现在现行信息安全技术和处理方法中的某些脆弱性的信息，以及有关现行信息安全技术无力解决的某些脆弱性的信息。尚未得到重视的脆弱性前馈信息，将给定义信息安全技术差距的任务打下一个基于关键基础设施信息技术现状“事实”的基础，同时还能帮助这些任务进一步搞清由关键基础设施运营者越来越多使用信息技术而带来的需要。定义这些差距，其实也就是为旨在弥补这些差距而进行的信息安全研发工作定义目标（见图 9-1 中右上方正数第二个蓝色框）。与近期研发工作的结果一样，这些在技术上付出的努力会为关键基础设施保护带来新的信息安全技术。

脆弱性信息将为关键基础设施 IT 运行的改进产生立竿见影的结果（见图 9-1 左中部的橙色框）。

脆弱性信息还将为定义现行信息安全技术处理方法和政策差距的任务提供第二类前馈信息。定义这些差距，其实也就是在定义一系列研发工作的目标：定义信息安全处理方法和政策，用以提高关键基础设施运营者运用现有信息安全技术的能力。这种工作的结果为关键基础设施运营者以及相关具体部门在信息安全方面提供了指南。如图 9-1 右下部分所示，这些指南由三种结果构成：有关如何运用现有信息安全技术满足关键基础设施需要的指南、有关用于管理信息安全技术和相关安全问题（如信息技术资产的物理和流程安全问题）的合理的处理方法和政策的指南、有关以前一致且可重复的方式通过比较结果而进行关键基础设施 IT 安全评估的指南。

对关键基础设施运营者之间的运行性互依赖性而进行的第三类运行研究，可产生双重结果。第一种结果，是用以指导近期矫正措施（见图 9-1 左中部的橙色结果框），进而缩小连锁性攻击影响范围。第二种结果是实现面向 CIP 技术研发的目标，为关键基础设施的互依赖性建模，并为业务连续性计划提供帮助。这种研发工作的结果，将包括关键基础设施业务连续性计划指南（图 9-1 右下部所示第四类关键基础设施 / 部门指南）以及用来定义业务连续性计划需求并制定这些计划的指南。

#### 4. CIP 中的 InfoSec 技术研究领域

尽管由于我们对可用来定义技术差距的关键基础设施 IT 脆弱性缺乏足够了解，迄今还没有正式进行过安全技术差距研究，但是对关键基础设施 IT 计算的一般性了解向我们提示，在 InfoSec 的若干个领域必须开展研发工作。这些领域的研发可以促使我们勾勒出比较完整的关键基础设施研发需求图，这个研发需求图来自于（对关键基础设施的）运行研究，最终可加强业界人士对关键基础设施脆弱性的了解。本章列举了研发的几个领域，其中有的工作还没有开展过，有的工作虽然已在进行之中，但并不是以满足关键基础设施保护的需要为目标的。

## 跨机构的安全

要想打破第2章描述过的单一所有者/运营者模式，就需要开展有关跨机构安全的研发。目前，这方面的研发工作称得上凤毛麟角，而且是直到最近才开始有人进行的。常用的商业措施，如不同系统的连接、电子商务基础设施的共享、供应链的管理等，其发展速度远远超过了可投入商业应用的安全技术和当前进行的研究工作。这方面的技术研发有大量工作要做，其一大目标应该是，确定与关键基础设施运营者网络互依赖性及连锁性攻击相关的脆弱性。随着网络边界变得越来越模糊、跨越这些界线的应用和交互运行变得越来越复杂，本章小标题所列的研发领域数量也在不断增多。关键基础设施运营者无一例外地都要面对信息技术日渐复杂的发展趋势。

研发工作中一个内容特别丰富的领域是应用得越来越广泛的“网络服务”模式，这种可供多方跨机构运营的模式，是通过最近的一些新技术（如 Enterprise Java Beans、Java 服务器网页、主动服务器页面和应用服务器）建立起来的，这些技术仍在基于 XML、UDDI、SOAP 和其他不断发展的标准和技术来增加新功能。研发工作在这一领域具有很大施展空间，所产生的安全技术可对涉及范围越来越广的跨机构计算技术进行管理，强制性限制一个机构对另一机构资源的访问。就关键基础设施保护而言，每个具有依赖性的关键基础设施运营者，都应受限于只能最低程度访问合作伙伴的系统，对合作伙伴系统的使用必须得到许可，方可转入自动运行模式。由于存在着连锁攻击的威胁，对于关键基础设施服务提供商来说，这种最低权限限制尤其具有重要意义。

## 基于异常的自适应安全监控

基于异常的安全监控是对当前使用的入侵检测系统（IDS）的一种必要补充。现行 IDS 技术所基于的是用户十分熟悉的一项抗病毒技术：保存和更新已知攻击的数据库；搜索发生攻击的情况，将其与数据库中的所有项目进行比较。这种通过把网络流与已知攻击标识进行比较而达到监控目的的 IDS 手段对及时更新数据库提出了很高要求。也就是说，每个 IDS 系统的工作标识必须不断更新才能跟得上网络级攻击技术的不断发展。这方面的残余风险是，一个组织的 IT 系统在一次新的攻击被识别并且创建标识和进行分配之前，很可能就已经受到了破坏。此外，在创建新标识与将其分配到某一特定 IDS 部位之间，还存在着时间差。尽管很多企业可以接受这种残余风险，但是对于关键基础设施运营者来说，这样的情况绝不允许出现。

与此相对照，基于异常的安全监控所依据的是现行策略或规则中有关得到允许的网络流模式的概念。这种手段具有一种独特优势，即不等潜在恶意行为发生就将其识别出来。任何不符合规则的行为都构成了发出预警的充分条件，甚至还应做出响应，封闭不符合规定的网络流。

## 不同类型数据的融合

任何安全监控技术的价值都取决于它所使用的种类范围极广的原始记录的数量。在大多数典型的网络中（其中包括关键基础设施运营者），数据量都十分巨大。因此，对于设计能够以每秒数千兆字节的速度实时处理细节的网络级数据包的系统来说，研发工作面临着严峻的挑战。即便这样的挑战问题得到了解决，安全监控系统的分析组件也要与整个系统完全匹配。还有更大的挑战在等着我们，那就是，如何使用众多种类型的与安全相关的记录数据。

仅仅对网络级数据进行分析，还不足以检测出会对得到允许的数据通道和应用交易造成破

坏的安全隐患。网络级数据会因同一网络监控组件内的应用级协议检查而不断增加。然而，对关键性应用数据流作彻底检查需要耗费大量精力，而且在很多情况下也是完全没有必要的，因为在相关的一系列典型系统中，与安全有关的记录数据称得上浩如烟海，其中既有应用级交易记录，也有来自各种典型关键基础设施组件（如应用服务器、网络服务器、DBMS 服务器等）的数据记录，以及服务器主机和 workstation 主机上的操作系统记录。

基于如此大量数据的安全监控 / 分析具有巨大的潜在好处。但是迄今为止，在出于给分析技术做统一数据输入的目的而在不同类型数据上做到前后一致的简化记录并进行数据融合方面，却几乎没有进行过任何研发工作。这类技术包括以检测与异常行为模式相符的行为或与正常行为模式不相符的行为为目的的基于配置、规定、策略、模式等的分析技术。

除了数据类型的多样性外，数据融合也潜在包括了涉及大量联网系统的大规模数据源样本，因此也称得上是一种挑战。在典型的网络体系结构中，存在着很多典型的“存储区”（面向互联网的边界网络、面向 VPN 的企业外联网、远程访问设施、工作站的聚合层、部门网、“服务器群”的分配层、“服务器群”的集群层、存储区网……）。每个区都有各自不同的活动，涵盖这些活动类型的数据聚合可以使分析系统能够将发生在网络各个不同部分中的不同类型事件关联到一起。

### 数据挖掘和审计简化

合成后的网络/系统/应用实时监控和分析可以成为一种重要的手段，来检测和隔离安全异常情况，以预防大规模安全事件，特别是对上述数据融合和分析的研发取得硕果的时候。然而，安全意外迟早都会发生，计算机取证分析工作也必须进行。在实时分析历史数据的过程中，事后分析日志肯定会大量涉及归档的静态数据。因此，把现有的和新涌现的研发成果应用到旨在解决计算机取证分析问题的大规模数据挖掘中，会有巨大的潜在好处。

当前，大量与安全有关的日志数据无人理会，原因就在于缺乏工具对它们进行分析。但是，如果开发出了这样的工具，有效的安全态势还应包括对审计日志的缩减和安全分析，以发现被巧妙伪装的攻击和蛰伏的攻击。这种做法可以在意外事件发生之前以计算机取证模式通过用定期统计分析来补充实时分析的手段改善安全态势。

在眼下的商业活动中，很多安全意外事件都是在最初的故障出现后的某个时刻被发现的。这种情况虽然并不理想，但是在业务计算中却是可以接受的，因为攻击造成的后果中并不包含影响企业的任务职能的基本故障。但是关键基础设施系统的情况就不是这样了。此外，当前常用的事件响应方法（通常既费钱又耗时）对关键基础设施系统可能不会奏效。应该在此强调的是，要想对攻击进行准确分析，并决定应该采取何种行之有效的响应方式，就需要有效果更好的数据挖掘技术。

在实时分析方面，数据挖掘在一定程度上面临的是数据类型分布极广的潜在挑战。尽管 IETF 的早期工作开发出了可以解决常见格式问题的标准数据格式，但是迄今为止，在利用其他与安全相关的常用数据格式（如 CIFS）来从安全研发领域之外推动数据挖掘技术研发工作开展方面，却几乎还没有任何人做出过努力。

### 快速响应：系统重建

系统重建也是安全事件响应的一个重要组成部分。遭到破坏的系统必须用备份和原始媒介重建，先是把系统重建到一种安全初态，然后是恢复操作、重装软件、重新配置以及其他相关

活动。在现行的事件响应手段中，这些工作全都既耗时又费钱，而且现行手段并不足以满足关键基础设施的需要。

要想满足关键基础设施受攻击后快速重建的更为严格的需要（并且为整个商业计算带来好处），就需要有适于大规模系统级检查点 / 回退交易的技术，并能适于绝大多数系统的整个系统状态。对于关键基础设施来说，这样的快速重建极其重要，它可以用作重新建设整个系统的替代性措施。

除了高度自动和快速外，计算机取证分析也是一种关键性要求。当今，计算机取证工作往往由于遭到破坏的系统为了调查目的必须保存下来而争执不下。虽然有些极为关键的系统有备用或热备份系统可供计算机取证使用，但是并非每个系统都适于拿来做对照分析。因此，自动化的系统重建技术可能需要包含对整个受破坏系统进行检查的手段，从而使受破坏系统得以为了计算机取证的目的而重建。

### 适于信息共享的分布式系统安全

信息共享和分析中心（ISAC）使关键基础设施运营者得以实时共享与安全相关的信息，同时也为其他形式的合作提供了一个论坛。<sup>①</sup>但是信息共享和分析中心本身也有其不可忽视的信息安全需求。信息共享和分析中心的信息库极具价值，这不仅对于传播信息并且依赖有效的匿名和其他形式的保护的 ISAC 成员来说是如此，而且还因为关键基础设施运营者的脆弱性信息对于敌对分子也非常有用。

信息共享和分析中心承受的风险还不仅仅限于它的信息库。敌对分子可能会利用信息共享和分析中心的计算基础设施攻击其成员公司。例如，一个信息共享和分析中心可能含有用于其日常业务的专用系统和/或网络连接。成员公司可以通过网络连接进入这些系统，而反过来，有人也能通过信息共享和分析中心的系统进入成员公司的网络。作为选择，信息共享和分析中心的业务可通过成员之间的跨机构计算进行，最初或许通过通报的方式，但最终还是要落实到应用之中。这样的通信渠道和业务流程会遭到敌对分子破坏，攻击行为可以从一个关键基础设施运营者开始，由此波及信息共享和分析中心的其他成员，从而形成连锁性攻击。

因此，信息共享和分析中心应被视为一种关键性国家网络资产，应该对其实施严密的网络保护措施。眼下，我们没有理由认为现行信息安全技术不足以满足信息共享和分析中心当前的要求（将来可能会需要研发一些具有特定目标的安全机制，以实现脆弱性和潜在事件信息的实时共享）。然而，随着信息共享和分析中心基础设施规模的不断扩大，其复杂程度越来越高，有关信息安全的问题，如了解问题的复杂需要、授权要求、通过授权控制跨机构和信息共享和分析中心内的数据流等也会变得更加复杂。各信息共享和分析中心之间的信息共享、跨部门的信息共享以及信息共享和分析中心与公共预警论坛和国土安全机构的网络部门之间的合作，也存在同样的问题。

### 互依赖性分析

为关键基础设施互依赖性进行建模的分析技术构成了虽不涉及信息安全本身但却对关键基础设施保护十分重要的技术研发工作的一个领域。很多关键基础设施运营者都面临着产生于

---

<sup>①</sup> 例如，信息共享和分析中心可能会受 FOIA 的保护，使关键基础设施运营者“比较”有关安全评估、脆弱性、矫正技术以及工作合作的“说明”，最终在合理的实践措施和改善整个部门安全状况上达成一致。

相互依赖的风险，其中很多风险是可以大大降低的。但是，确定以最具成本效益的技术来最大程度地降低某一特定关键基础设施保护预算的风险，是一项非常复杂的任务。关键基础设施运营者之间的各种互依赖性十分复杂，在大多数情况下，进行互依赖性风险分析所面临的困难以及分析结果的不确定性，几乎抵消了分析工作所可能带来的好处。此外，很多情况下的风险都来自于外部（一个关键基础设施运营者对另一运营者的依赖，所形成的风险便是：对另一运营者的攻击会对第一个运营者产生连锁影响，而且后果是系统性的而非局部性的）。也就是说，一个关键基础设施运营者的功能受损（或许是另一运营者功能受损的连锁性结果）是整个系统遭到破坏的一个组成部分，而对这个运营者采取矫正措施，也会对依赖该运营者的其他关键基础设施运营者产生连锁影响。

因此可以说，针对自动协助关键基础设施运营者以最有效方式调整自己对其他运营者的依赖，要对现有的进行运行管理和后勤保障的优化，这为我们提出了清晰的研发需求。为关键基础设施互依赖性建模的分析工具是不可或缺的，首先要用它们开发出系统和依赖程度模型，然后通过它们制定出如何改善后勤保障以缩小攻击的连锁影响范围的计划。这样的工具不但对基础设施运营者化解风险至关重要，而且还会对整个部门乃至整个国家带来好处。我们不妨想象一下，如果最终能够就国家最重要的关键基础设施系统开发出一个完整的模型，用以确定互依赖性“节点”和/或有可能产生连锁影响的共同风险，那会带来什么样的结果？这种节点代表着针对攻击影响的“最高回报”，无论攻击是物理性质的和还是网络恐怖主义性质的，抑或是两者兼而有之的。

由此可见，这一领域的研发工作有可能在地区乃至国家范围内得到巨大的回报，关键基础设施运营者得到的新工具将使他们能够明智且合理地把资本资源投放到特定的冗余性组件或计划中的快速恢复上，从而取得减缓风险的最佳效果。在地区和国家层面上，开发出来的模型将能识别关键节点并合理配置后勤保障投入，这一领域的目标与关键基础设施运营者相同，只是规模更大而已。

## 5. CIP 中的 InfoSec 运行研究领域

运行研究包括去核对并分析各代表性的关键基础设施运营者的信息安全态势信息，旨在标识存在的差距，以定义近期的需求，从而制定合理的实践措施，或定义出长期的技术研发需求。关键基础设施保护运行研究是研发项目中必不可少的一个重要组成部分，如本文第 1 章所述，研发规划会因人们对关键基础设施 IT 系统现存脆弱性缺乏了解以及对现行信息安全技术对解决脆弱性问题的有效性和实用性缺乏了解而受到阻碍。在当前网络恐怖主义猖獗的背景下，这种认识不足所带来的后果是不可忽视的，很多关键基础设施运营者的 IT 系统就是在没有被看作重要国家资产的情况下创建起来的。确实，有些运营者当前的活动及其拟提高自动化程度和扩大信息技术应用范围的有关计划，并没有对原始的系统做出任何改变，而这些原始的系统是人们在未将基础设施视为关键资产之前就部署的。

### 运行研究中的差距分析

由此可见，在从后勤保障和技术角度加强我们对关键基础设施运营者运行工作的了解方面，还存在着通过运行研究填补巨大且关键的差距的迫切需要。“现今实情”对于评估我们的

关键基础设施在网络恐怖主义威胁下的脆弱性来说，称得上至关重要。当前，有关这些脆弱性的信息只存在于一些曾经进行过安全评估的基础设施运营者严格保密的文件中。没有人真正了解所有公司和部门共有的脆弱性。由于我们国家的关键基础设施大多由私营公司运营，没有人知道这些脆弱性的表现频率有多高、到底具有多大的普遍性。也就是说，没有人知道现行信息安全技术和处理方法到底有什么缺陷。

运行研究由与基础设施公司共同了解它们是如何运营其 IT 系统的工作构成。分析工作通常侧重于每个外部网络接口的特性和原理、用以评估系统控制和对正确运行控制系统至为关键的数据的网络体系结构、专门用于控制系统的安全机制和处理方法等问题。一定数量的运行研究可以在 PCIS 的指导下进行，用以帮助那些典型或极为关键的基础设施成员公司，同时还能对与合作组织有关的其他公司开展的运行研究工作提供支持。

这样的运行研究任务通常有两大重要目标：为安全技术差距研究提供信息；为关键基础设施运营者的脆弱性评估定义度量尺度、标准、准则和方法。向安全技术的差距研究和安全实践措施的差距研究输入信息是不可或缺的一步，因为这类研究的基础是使用 IT 的真实基础设施组织的典型情况。因此，第一个目标也就是努力开发一个研发项目。然而第二个目标的规模要更大。当前，评估和改善关键基础设施信息安全的工作困难重重，原因不仅在于我们在了解情况方面存在差距，而且还因我们缺乏有关信息安全的专业知识（尤其是在迄今还没有被认为是关键性国家资产的关键基础设施的某些方面），同时也因为我们对关键基础设施计算中的信息安全现状知之甚少。由此可见，就针对基础设施组织的 IT 系统进行可重复和可比较的脆弱性评估而言，通过运行研究而定义度量尺度、标准、准则和方法是具有巨大的潜在价值的。需要再次强调的是，基于现实世界中关键基础设施 IT 的实际情况开发这些工具至关重要。评估工作越方便、越标准、越可重复，它就能越不断地改善信息安全态势，同时也能越频繁地展示研发工作中的技术差距。

### 研究领域

运行研究涉及三个可相互分离的领域。第一个领域侧重于信息安全态势、脆弱性和关键基础设施运营者 IT 系统中未被满足的信息安全需要。第二个领域与第一个有些类似，但专门侧重于 IT 互依赖性。第三个领域则涉及非 IT 的互依赖性，所侧重的是关键基础设施运营者之间及其与合作伙伴和提供商等外部实体之间在功能性和运行性互依赖性。第三个领域的研究结果由用于近期消除互依赖性风险的典型方法以及为互依赖性研发提供的信息组成，后者包括但不限于本文第 4 章“互依赖性分析”介绍的内容。

第二个领域的运行研究的结果是关键基础设施中跨机构计算常见的互依赖性信息以及关键基础设施中某些可能的特定需求的信息。这一领域研究的一个重要项目涉及关键基础设施运营者之间计算（这种计算有别于诸如运营者与提供商之间的其他计算）中的安全技术和实践措施。在关键基础设施运营者之间，由于他们存在着互依赖性，网络基础设施、通信和应用可能会有截然不同的安全和信息要求。也就是说，相互依赖的关键基础设施运营者可能会互相带来关键基础设施保护的脆弱性，而运营者与提供商之间的计算只会产生单向的关键基础设施保护风险，即通过与提供商之间的计算对关键基础设施运营者构成威胁。因此，研究结果应对以下问题做出解答：

- 现有安全技术足以满足关键基础设施运营者与提供商之间计算的典型安全需要吗？



- 现有安全处理方法足以满足关键基础设施运营者与提供商之间计算的典型安全需要吗？
- 现有安全技术足以满足关键基础设施运营者与其他关键基础设施运营者之间计算的典型安全需要吗？
- 现有安全处理方法足以满足关键基础设施运营者与其他关键基础设施运营者之间计算的典型安全需要吗？

第一个领域的运行研究的结果与第二个领域的结果类似，但是更侧重于关键基础设施运营者的内部 IT 运行。与第二个领域一样，第一个领域的运行研究应该标识出常见的脆弱性和安全差距，同时确定现有信息安全技术能够解决哪些脆弱性和差距问题，又对哪些无能为力。除了有关研发差距和可行的近期矫正措施的信息外，研究结果还应就针对关键基础设施保护的工具体研发提出要求。这些涉及范围极广的工具应包括合理的实践措施、信息安全技术应用指南、信息安全政策和流程模板以及用于关键基础设施保护信息安全脆弱性评估的标准工具。

### 结果总结

实施有关关键基础设施信息安全和关键基础设施互依赖性的运行研究后，将会得出以下几类具有实际意义的结果：

- 更准确地了解脆弱性；
- 确定与信息安全技术、产品、处理方法和流程有关的有效近期矫正措施；
- 开发可应用到关键基础设施系统之中的 InfoSec 通用指南和标准；
- 开发用以评估关键基础设施系统所需遵循的指南和标准；
- 定义未被现有信息安全技术和实践措施满足的关键基础设施安全需求；
- 评估未被现行研发工作满足的需求，定义现行研发工作的差距。

请注意，这些“指南”（现有信息安全技术应用指南、所提议的政策 / 流程、评估准则、矫正指南等）在某一关键基础设施部门内或关键基础设施服务提供商中应是标准性的。然而，如果没有这些指南，关键基础设施运营者开展安全评估和矫正工作会遇到很大困难——提供标识实践措施的差距和技术差距所需的信息会大幅度减少，而这些差距是要通过与关键基础设施运营者的需求始终相关的研发工作来填补的。因此，这些活动——评估、矫正和差距分析的前后一致性显得尤为至关重要。

使安全能力达到一般水平是特别重要的一项需求，因为关键基础设施中的互依赖系统存在着最脆弱的连接问题。一个安全隐患比较严重的关键基础设施运营者不仅在单一的攻击中会显得非常脆弱且会造成连锁性附带损害，而且会在多重连锁电子攻击中弱不禁风且造成波及面很广的连锁性附带损害。要想降低这种极其脆弱的连接风险，技术和实践措施这两个方面缺一不可。信息技术（其中包括安全技术）是必不可少的，但又不足以解决全部问题。每个关键基础设施运营者都必须运用安全技术来满足其所面临的安全需求，同时还必须通过妥善使用、操作和维护所采用的系统才能确保其始终高效运转。

最后需要注意的是与运行研究和研发差距分析密切相关的政策问题。在全国范围内改善关键基础设施网络安全状况需要政策决策和政府的参与。这种参与几乎肯定应该包括政府对关键基础设施保护中 InfoSec 研发工作的资金投入以及对规模越来越大的关键基础设施保护研发工作进行协调的资金投入。在这些方面的努力要想结出硕果，就必须与关键基础设施的计算有高度关联性，运行研究的目的在于此。但是，政府的参与可能还应涉及推动关键基础设施网络

安全工作的发展，其中包括更多的是关键基础设施运营者开展安全评估、实施近期改进措施并设置强有力的信息安全项目。如本文第2章“政府政策问题”一节中所述，在全国范围内对这些领域的资金投入是一个极其重要的政策问题。但是，如果关键基础设施保护业界不能合理地相信现有的工具（正确合理的实践措施、评估指南等）对关键基础设施保护的强针对性——它们极可能提供可重复的结果，值得为之投入精力和资金，那么解决这个问题将会十分困难。

此外，按照这样的方针在全国范围内做出的任何努力都会不可避免地依赖于各关键基础设施部门之内和之间的协同合作，其中也包括各信息共享和分析中心在内。所以可以说，解决这些政府政策问题在很大程度上取决于公共-私营部门的合作活动，因为为提高关键基础设施保护水平而定义和使用现有工具的机构，正是关键基础设施运营者及其工业组织，这些工具可使任何公共-私营组织为提高关键基础设施保护水平而做出的努力，结出丰硕的果实。

## 6. 总结

开发关键基础设施保护研发项目，在很大程度上取决于我们是否能填补对关键基础设施安全态势的认识不足，以及能否认识到可期望被 CIP 研发工作解决的待决需求。尽管现有信息安全技术已经在很多关键基础设施部门投入使用，但是日趋复杂的 IT 应用正在使信息安全技术的发展步伐大大落于当前计算实践。如果不针对关键基础设施保护做出协调一致的努力，信息安全技术就会无法继续满足关键基础设施保护的需求。可行的近期工作包括发展 R&D 工作、增强项目合作、开辟针对关键基础设施保护的信息安全研究新领域或扩大研究范围（本文阐述了其中部分领域的研究）、开展关键基础设施中应用型 IT 所需的安全运行研究。应该强调的是，运行研究产生的结果还有助于大幅度改善关键基础设施的信息安全状况，同时还有助于推动解决政府政策问题。

技术性研究和运行性研究都具有不可忽视的重要意义，因为当今最紧迫的 CIP 安全问题是抵御网络恐怖主义分子与物理基础设施恐怖主义分子联合发起的攻击。无论从行业还是从国家角度看，我们正努力认识和解决的安全问题将帮助我们预防、保护和减缓对我们关键基础设施的破坏。网络攻击与标准的恐怖主义活动相结合后，不仅会增加物理攻击的效果和成功率，而且会增加混乱，引发物理破坏和伤亡。随着我们的系统，包括电子系统和运营系统越来越复杂，相互依赖得越来越紧密，地理触及面越来越广，遭到连锁性破坏的风险和面对攻击时的脆弱也在与日俱增。我们所面临的是涉及范围极广的威胁。每台与互联网相联的计算机都能把风险扩大，而这种状况还在不断发展。

要想不断提高我们抵御这些威胁的能力，网络空间安全研发的综合性基石中就必须包含差距分析和具有前瞻性的研发工作。由于各种解决方案的设计都必须旨在解决我们的复杂现状中的具体问题，关键基础设施保护的研发工作必将加深我们对如下问题的认识：什么类型的攻击会令我们不堪一击？有哪些行之有效的系统可供我们使用？我们的工作缺少哪些环节？我们怎样才能化解风险并消除我们国家的 IT 在网络攻击下表现出来的脆弱性？

---

## 十、银行与金融部门关键基础设施保障国家战略（摘要）

（第 1.0 版）

美国银行与金融部门  
2002 年 5 月 13 日

---



扫二维码阅读全文

## 执行摘要

美国的银行与金融部门肩负着保卫 21.5 亿信用资产的重任。它体现在个体客户的信用资产的整体信托中，与这些资产的安全性、保密性、完整性和可用性密切相关。这种信托往往容易出现偏差。良好的信托状况依赖于国家经济基础设施的强劲生命力。该基础设施必须具备对于来自物理和网络空间的威胁和攻击的抵抗力。只有美国政府能够保护国家经济基础设施。银行与金融部门为了准确地理解部门责任，已经制定了用于保护国家基础设施关键部分的国家战略。这个战略将指导该部门发挥部门功能和利用部门资源，以此完成部门责任。

为确保客户信托和安全服务的持续性，银行与金融部门已经投入了很多资源。通过利用早期的准备工作和与工业界广泛的合作，国家战略将努力在指导未来任务时合理使用现有的可用资源，对本部门的工作进行战略性规划。

这份战略不仅是一份重要的本部门工作指南，也是对布什总统相关管理政策的推进。为解决关键基础设施问题，他曾经建议联邦政府和国家以及地方政府进行合作。本文的根源可以追溯到 1998 年 5 月发布的第 63 号总统令（PDD63）。银行与金融部门由社区银行、信用合作社、大型综合服务全球控股公司、安全和保险公司、交易汇总中心、支付处理中心、中央交易机构、自律性组织（SRO）、票据交换以及其他中间机构共同组成。

本文指出国家银行与金融部门的任务是在和平年代和威胁发生的情况下确保提供可靠的部门服务。在很大程度上，美国经济基础设施所必须具备的强大、持续的生命力取决于银行与金融部门在识别、防范和预测物理与网络空间威胁方面所具备的能力。本部门一旦受到威胁，将严重降低联邦、州、地方和私营实体履行其义务的能力，从而无法确保国家经济工作的有序性。这些威胁将会影响关键的债务、信托、支付、资产保管和本部门为广大客户、企业和政府部门提供的风险转移服务。

随着美国步入 21 世纪，银行和政府部门在国内和国际上面临的物理和网络空间威胁将继续增加。威胁范围固有的复杂性将导致银行与金融部门必须重视有关威胁和事件处理的四个关键方面，即：

- 金融服务被破坏的可能程度；
- 部门干预的时机；
- 部门交流的过程；
- 服务重建。

针对以上问题，为了缓解风险并实现目标，我们确定了指导本部门工作的四条首要原则：

- 检查银行与金融部门的核心基础设施，确定和评估具有系统化风险的领域和暴露点。
- 核心基础设施的所有者和运营者必须使用合理的风险管理、业务和安全措施，并参与到基础设施保障的统一规划工作中来。
- 核心基础设施的所有者和运营者要行动起来，并在必要时以合作的方式相互保护和联合防御，以此防范系统风险。
- 联邦政府要与核心基础设施的所有者和运营者合作，在必要时及时响应并防御这些基础设施面临的系统威胁。

在国家战略中，以上四条原则有助于形成对部门计划和执行工作进行指导的框架。通过使

用合理的业务措施、信息安全原理和严谨的风险管理政策，部门将不断在确保信誉上加强力度，主要体现在：

- 评估与理解：分析基础设施的力度、相关性、脆弱性和解决虚拟与物理问题的能力。
- 准备、防护和恢复：逐步加强部门预防风险、防御威胁和在金融和技术方面从遭受系统攻击的状况下进行恢复的能力。
- 检测和响应：制定并执行检测政策，及时响应银行与金融部门信息基础设施面临的攻击。
- 重建和恢复：具备将技术和金融的服务、功能恢复和还原到其正常运行状态的能力。
- 金融风险管理：具备在金融上抵抗攻击及其影响的能力。

要使本框架成功有效，就需要整个银行与金融部门在网络空间和物理基础设施的事件上采取合作的态度，共同检测、响应和恢复。这就要求协商和合作不仅限于传统银行与金融部门的成员（包括保险业），而且包括该部门的提供商、服务商、法规制定者。进一步说，银行与金融部门要认识到，单凭一个独立机构或部门独自孤立地响应现在及未来的威胁是不可能的。因此，部门中的很多成员越来越注重部门内和部门间的合作。当前，银行与金融部门的合作要求对关键态势的准备工作 and 规划必须基于公共-私营合作的整体响应。了解了这一要求，所有部门的计划就必须协调统一地凝聚在国家战略中。

而且，银行与金融部门的国家战略还建议采取一系列应该采取的行动。为了实现国家目标——提供可靠服务，建议首先进行评估，确定部门的核心基础设施和部门中面临系统化风险的可能领域。其他行动还包括：

- 设计和建模（经济模型、数学模型等），评估和理解系统安全问题对银行与金融部门的影响。
- 实施意识战略，对部门的成员、相关利益团体、执行董事会进行教育和推广。
- 鼓励采用保险等风险管理技术，缓解网络空间攻击造成的影响。
- 与政府一起设计和实施共享的协调管理过程，以确保能够检测并响应基础设施面临的系统化威胁。
- 探索资金选择，确保以上的部门活动正常开展。

商务部门、公众和政府团体间的广泛支持和合作对不断变化的美国及全球经济都是积极有效的。随着政府和关键基础设施部门间的相互合作，银行与金融部门将在 2002 年年底集中实施所声称的本部门行动。本篇国家战略将指明成功完成这些目标的原动力和任务。

## 1. 银行与金融部门透视

### A. 部门组成和行业动力

银行与金融部门是负责美国经济健康发展的综合体。美联储汇报告表明，2001 年第一季度，美国金融机构持有的信用市场资产高达 21.5 亿美元。金融机构中最大的几类机构包括商业银行（5 亿美元）、保险公司（2.5 亿美元）、共同基金（2.5 亿美元）、政府资助企业（1.5 亿美元）、养恤基金（1.6 亿美元）和互助储蓄银行（1.5 亿美元）。其他资产分别由抵押公司、证券经纪人和交易人等金融机构拥有。

银行与金融部门的组成已经超出了以上公司的范围，它还包括基础性的专业化服务机构及

服务提供商组成的网络，这些机构和提供商为了使本部门能够提供可信服务环境而提供了支持。这个网络包括证券和商品交易网络、资金转账网络、支付网络、清算公司、信托和监护公司以及信托和信息系统。在第三方提供商提供的系统和应用程序、硬件和软件以及技术服务的帮助下，银行与金融公司也越来越倾向于对某些任务实行外包。虽然这些第三方服务提供商并不是传统意义上的银行与金融部门成员，但它们已然成为银行与金融基础设施中不可或缺的一部分。

除了那些协助银行与金融部门运行的公司和服务机构外，某些行业发展方向会对本部门缓解风险的能力造成重要影响。这些发展趋势能影响业务活动的开销、业务运行的环境以及部门的未来发展方向。通过初步确定这些趋势以及预计其在未来所具有的重要作用，银行与金融部门在最大可能地利用本部门的能力的同时将得以安全发展，呈现欣欣向荣的景象。这些发展趋势包括：

- 技术更新；
- 合并；
- 全球化；
- 重组；
- 分布式技术；
- 多种渠道；
- 公共基础设施；
- 互依赖性。

#### **技术更新**

计算机和网络资源及其服务对已知和尚待发觉的脆弱性越来越敏感。除非技术提供商在设计、测试和生产时就极力强调产品的安全性，这一趋势将会持续。使用“补丁”的挽救措施不会彻底地缓解风险。

来自“网络空间”的威胁和脆弱性是本部门面临的最大挑战。从 21 世纪初开始，网络空间的脆弱性和犯罪便以指数形式增长，而且这一趋势将与技术的使用程度和依赖程度的增长成比例增长。金融和银行部门必须以一种灵活而有效的方式，在维护这些技术的运行并提供信息传递服务的稳定性物理状态的同时解决这一趋势。

#### **合并**

全球的合并趋势同样导致了银行与金融部门的大量并购，导致资产越来越集中，需要较少的支持服务。这种仍大行其道的方式可能会在个体机构遇到麻烦的情况下，特别是在接下来的跨公司整合过程中，增加金融系统面临的风险。

#### **全球化**

金融交易和活动无时无刻不再进行，没有政治和国界之分。无处不在的 Internet 使客户、契约方、仲裁人、主要协会等可以在全球范围内不间断地合作和交流。银行与金融部门将经历更多的跨国跨文化的合作，这将为国际舞台引入额外的风险和脆弱性。

#### **重组**

金融机构正在不断地削减冗余的项目和设施，简化系统和过程，并在整体上减少个人开支，

这些都有可能增加风险。设备集中使得我们严重依赖于少数站点，因此任何一个站点的损失都将带来比以往更大的影响。集中让我们不得不更依赖更少的人，更复杂的系统和程序，增加了单一组件失效所带来损失的可能。人员精简使被迫离开的员工产生报复心理，同时留下来的员工也会有一定程度的不满和想法。

### 分布式技术

传统上是对中央计算机系统采用物理和逻辑访问控制，对高级设备的有效性采取保护措施。随着客户端服务器和开放源码系统在越来越多分散的缺乏管理的环境中使用，由未授权入侵缺乏保护的设备、远程系统和网络的行为所造成的风险会不断增加。这将导致数据的损坏、系统无效及丧失对网络和计算机系统的控制。

### 多种渠道

金融服务已不再局限在传统“砖瓦”砌成的办公室中，而是更多地通过传送通道提供。机构系统的进入点增多导致脆弱性个数的相应增长，如卡式激活终端、有线和移动电话、手持装置。这一趋势增加了错误认证和非授权访问为封闭的内部网络系统带来的风险。

### 公共基础设施

金融机构在接收和传输信息、处理交易和向客户提供服务时增加了自身对公开共享数据网络的依赖（如 Internet）。相对于专属或租赁专用网络，公共共享网络更缺乏安全性。

### 互依赖性

银行与金融部门在基本服务和专业化服务上越来越依赖第三方服务提供商。基本服务包括通信和电力，专业化服务则更加多样和更加分布，包括外包信息和数据处理、使用外部系统和应用软件、由外部公司对有关全球金融市场的复杂信息进行预处理等。

这些趋势源于银行与金融部门使用的开放网络系统在不断增长的现实情况，并对取代单个机构内的传统封闭的私营系统起到了推动作用。引用首席信息安全和隐私官员 Steve Katz 在 1999 年 3 月的一段话可以说明有关技术转移的安全问题：

“从安全角度看，最重要的一点是，越来越多的公司迫切地邀请其客户直接或通过在线链接访问产品产地——也可以叫作厂房。这是 Internet 上增长最快的部分，而滥用行为，即访问其他可能是公司封闭领域内容的行为一定会给很多客户带来风险，无论是知道的还是不知道的，希望的还是不希望。这一积极地在线公开趋势使安全模型转变为要求人们进来，而不是让人们待在外面。”

## B. 银行与金融部门正在专注进行的工作

### 概述

鉴于关键基础设施面临威胁的特性和潜在影响，为解决脆弱性问题，银行与金融部门必须积极制定联合解决方案。方案中必须解释单个机构的业务连续性计划无法涵盖的暴露问题。这样的合作将使工业界能在整体上解决由基础设施面临的威胁所带来的潜在影响。

为完成此项目标，我们已经迈出了很多步子，拥有了较长的关键基础设施保护历史和经验知识。本部门中的一些重要的活动包括：

- 建立金融服务信息共享和分析中心 (FS/ISAC)，共享有关威胁、脆弱性和事件的信息。
- BITS 产品认证项目（全名为 BITS 金融服务安全实验室），根据特定标准和产品轮廓

进行测试，以确定银行与金融部门的安全目标和要求。

- 美国银行家协会（ABA）和证券工业协会（SIA），致力于保护客户的数据、防止洗钱活动和认证金融交易。
- 在整个证券行业实施证券工业协会业务连续性计划。
- 用其他金融交易协会的活动来保护金融系统的关键基础设施，如设定安全标准和增加行业的需求意识。

为了确保这些自我管理行为能与规章指南及意图保持一致，银行与金融部门还要与法规机构密切合作。这些机构将持续为解决安全问题起到重要的领导作用，包括 SEC 和联邦金融机构检查理事会。后者由联邦储蓄保险公司、美联储、国家信用合作处管理局、储蓄监管办公室和现金审计办公室组成。

部门行动：在地方、州和联邦一系列等级上，银行与金融部门要通过公共-私营合作，与管理机构和政府实体一起解决有关的安全和基础设施问题。

如前所述，无论本行业采取何种预防措施，它仍可能遭受对手的攻击，从而使金融系统本身受到威胁。银行与金融系统的成员将以合作管理的态度合力制定用于对系统攻击进行标识和响应的过程。这部分内容在一定程度上要依赖于标准和传统性的防御、检测、响应和恢复能力。

## 部门项目

本行业中的领先企业和团体已经开发了一系列计划，来协助其成员响应基础设施的挑战。这些计划的基本内容包括对付洗钱、安全、诈骗、盗窃和其他特殊领域中问题的信息共享、教育和行动计划。在解决这些问题的过程中，各机构可以作为提高基础设施保障的主角。

### （1）关键基础设施保障国家战略

国家战略是一个重要的指导文件，是对布什总统国家安全管理政策的有力补充。它提倡公共-私营部门联合应对关键基础设施领域的挑战。总统在 1997 年 10 月发布的关键基础设施保护总统委员会（PCCIP）报告中指出，银行与金融部门对国家稳定至关重要。这份报告指出，国家经济越来越依靠计算机和网络信息系统及其辅助设备。PCCIP 建议制定一份基于公共-私营联盟和信息共享的综合项目，据此保护银行、金融和关键基础设施不受物理威胁和网络空间潜在威胁的影响。

1998 年 6 月签署的有关关键基础设施保护的 63 号总统令（PDD63）任命财政部为“领导机构”之一，负责与银行与金融部门合作，协助制定上述的综合项目。财政部金融机构办公室负责监督工作。在与部门代表会晤后，财政部长任命花旗银行首席信息安全和隐私权官 Steve Katz 为此行业的部门协调员。以下行业代表要协助其工作，肩负起自己的管理责任：

- Stash Jarocki，摩根-斯坦利公司的副总裁，主管信息共享工作，负责制定和执行金融服务信息共享和分析中心的工作。
- Rhonda Maclean，美国美洲银行高级副总裁兼董事，负责培训和意识教育工作。
- F.W.Gerbracht Jr.，Credit Suisse First Boston 的首席信息安全官，负责脆弱性评估工作。
- Charles Blauner，Deutsche 副总裁，负责研发工作。

### （2）金融服务信息共享和分析中心（FS/ISAC）

银行与金融部门是第一个响应第 63 号总统令建立信息共享和分析中心的部门。1999 年 10



月 1 日，财政部长 Summers 宣布金融服务信息共享和分析中心 FS/ISAC 正式成立，同时到场的还有证券交易委员会主席 Arthur Levitt、美联储副主席 Roger Ferguson、国家安全委员会 Richard 和工业界的经理们。

金融服务信息共享和分析中心是银行与金融部门对各种攻击行为采取防御措施的标志。借助于来自 100 多个信息源的输入和分析结果以及一些成员提供的入侵检测数据，该中心能够发现潜在的威胁和脆弱性，并采用 Internet 邮件、传真和纸张/电话留言等方式发出有关威胁和脆弱性信息的预警-通知。

该中心一个最重要的贡献是通过“趋势”文件帮助确定具有潜在缺陷或新威胁的领域。在最初的 3 个月、6 个月和 12 个月内，该中心会分别总结出威胁、事件和脆弱性的内容，并对新风险和潜在问题的领域提供必要的评估。该中心使银行与金融部门几乎实时的共享一般的和部门特有的信息与技术，提供早期脆弱性和威胁预警报告，并建立对每个个体机构基础设施的改变方式。除此之外，中心还配备了可提供 24 小时昼夜服务的网络空间应急响应小组。

下表是关于金融服务信息共享和分析中心特点和能力的摘要。

#### 金融服务信息共享和分析中心描述

- 金融服务信息共享和分析中心是制定和共享有关物理和网络空间事件、威胁、脆弱性、解决方案的信息的数据库。这种自愿提供的信息将在认证后以匿名的方式提交和共享，因此参与成员无须面对法律问题，也不必为操作错误承担责任。
- 金融服务信息共享和分析中心是由其成员运营的有限责任公司，成员包括美国的大型银行、证券公司、保险公司和投资银行。该中心不由财政部等任何一家美国政府机构出资和管理。财政部人员只是承担适当的联络任务。
- 金融服务信息共享和分析中心的数据来自于所有参与该中心的成员、公共-私营信息源以及政府机构。目前，已有 100 多个信息源成为合格的可用于分析和预警的依据。需要强调的是，该中心不提供针对客户信息的共享和存储。此外，财政部等任何联邦政府机构都无法了解该中心的信息输入和输出细节。
- 信息共享一般从政府到金融服务信息共享和分析中心，有时也从中心到政府，但这一举措仍在讨论之中。例如，中心已与五角大楼联合任务小组/计算机网络作战组织，美国特工处和 FBI/NIPC 讨论了此类信息交换协议。截至目前，政府只向该中心提供信息。目前已经针对一些联合研究和项目提出了议题。
- 中心在适当的时候要与其他行业的信息共享和分析中心进行信息交换。
- 金融服务信息共享和分析中心要求所有的金融机构成员承担报告犯罪行为的义务，以此确保对机构的计算机和信息系统的正当管理和合法授权。
- 金融服务信息共享和分析中心在几次拒绝服务攻击和计算机病毒攻击期间起到了显著作用。在 2000 年 5 月的国会上，美国审计总署表扬说，在现存众多的用来对信息系统威胁和事件进行防御预警和对抗的公共-私营机制中，金融服务信息共享和分析中心是最好的。

### 金融服务信息共享和分析中心能提供并辅助的工作

- 从国家和全球商业、公众、私营和政府信息源收集信息用于分析。
- 无论对成员还是非成员，信息提供方式都是以流水线方式从决策层到金融社区的各层自上而下，即 CEO、管理层、响应层、审计和安全管理层。
- 按照对国家的重要性，对事件进行分类。
- 判断能表现出明显威胁的事件。
- 察觉影响整个金融部门的事件，从最小至最大的金融部门实体。
- 为通信提供后勤支持。
- 提供最初的事件指挥功能。
- 协调部门响应。
- 协助事件调查：识别威胁源、脆弱性探测和可能的动机。
- 与政府机构接洽。
- 协调各机构间的响应：确定应立即采取必要措施来控制风险的步骤，确定恢复步骤。
- 协调恢复工作。
- 分析事件报告。
- 在适当的时候向财政部汇报。
- 宣布部门紧急情况。

该中心的另一项工作是为部门间的信息交换制定要求和过程。中心大力倡导事件、威胁和脆弱性对国家和全球安全有影响且必须对其适当重视的理念。以事件管理为目标，中心能够研究本国企业或全球跨企业范围的事件。同时，由于中心可以接收涉密和敏感的政府信息，因此它可以对这些事件进行深度分析，并利用包括电子邮件、移动电话技术、呼叫中心、Internet、传真等方式在内的强健的电子网络，或者其他任何新式的商业和政府的涉密系统发布有关信息。

部门行动：银行与金融部门将通过金融服务信息共享和分析中心，最大可能地从共享和分析信息资源中获益，并扩大和提高与政府及其他部门信息共享和分析中心信息资源的信息交换能力。

### (3) BITS 的工作

①BITS 危机管理工作组：其工作是通过改进预防工作和通信状况，提高其成员从企业范围的大灾难中进行恢复的能力。其工作内容包括高等级场景的设定、CEO 危机时刻的通信能力、共享业务实践措施和在危机时刻维护公众秘密中关键信息的能力。

②BITS 产品认证项目（正式名称为 BITS 金融服务安全实验室）：这是另外一项工作，它是 BITS 于 1999 年 6 月建立的圆桌会议式的金融服务技术组。BITS 产品认证项目可向企业和客户提供保证，确保金融部门使用的产品都是通过专业机构公平测试过的。合格的产品上标有“BITS 测试”标记。

BITS 产品认证项目设计并开发了适用于不同类型产品的安全标准。标准的开发过程得到了产品供货商、50 多家金融机构和私营企业专家的支持。这些标准为金融机构提供了一套面向业务软件产品的一致性安全衡量准则。BITS 产品认证项目还致力于开发与通用准则（CC）测

试和评估体系保持一致的安全标准，从而使 BITS 的测试可以通过任何一个 CC 准则测试实验室完成。

下表为 BITS 开发的安全产品类标准及其他 BITS 工作：

#### BITS 危机管理行动

- 这些行动的主要目的是预防灾难并能在大规模业务中断后对其及时恢复，以确保持向客户提供可靠的服务。其行动由以下内容组成：
- CEO 和 CIO 在危机时刻的及时通信：BITS 将临时建立一个虚拟会议厅和通信线路，CEO 或设计者应及时会晤，商榷对策。在需要时还可以包含其他部门的代表。
- 场景和事件管理：BITS 已开发了协调事件管理工作的场景，并在出现危机情况时对工作进行优先顺序排列。远期的要求是设计模型并对不同关键基础设施的互依赖关系了如指掌。
- 最佳业务实践：这个团体作为一个协作团队，可共享有关业务连续性计划的实践，并且在成员之间对事件管理过程进行整合。
- 关键信息通信：公众的信赖对于危机管理非常重要。BITS 将与其他行业组织一起开发并向公众传达清晰的、有建设性的和准确的信息，使公众了解到所有 BITS 成员机构均已具备了安全合理的环境。

#### 其他 BITS 活动

- IT 服务提供商：BITS 为开发了一个综合性的《IT 服务提供商联盟风险管理技术框架》，以此帮助本机构和服务提供商了解怎样提供一个更加安全的基础设施。该框架整合了现行所有的管理要求。
- 综合服务：BITS 将组织其股东为不同的电子业务活动建立适宜的基础。作为该基础的一部分，BITS 将为综合服务的建立安全的业务实践和指南。当新老金融机构进入银行机构的管理的部门时，可以采取《BITS 综合服务志愿指南》中的。指南涉及了业务安全实践、隐私、客户信息泄漏、数据反馈和管理等要求。
- 移动金融服务的安全：BITS 为无线通信和移动金融服务提供了最基本的业务实践，特别强调了安全以及端到端传输的可靠性。这种银行与金融部门与信息通信部门之间的合作为其他关键基础设施部门间的合作提供了榜样。
- 电子业务中的保险：BITS 将“电子业务保险差距分析矩阵”作为用于确定网络空间事件、组织影响、传统保险业差距或问题以及新型保险行业问题的工具。
- 减少诈骗项目：BITS 将动员行业中负责检查、借贷和 Internet 诈骗行为的高级行政人员，促使他们相互合作，共享成功经验，改善数据库，建立用于解决基础设施诈骗问题的业务实践措施。

#### （4）证券工业协会（SIA）的工作

SIA 的主要工作之一即合作开发用于灾难恢复的业务连续性计划。SIA 业务连续性计划委员会（BPC）的任务是：

- 为证券公司、行业组织和服务提供商共享特殊的业务连续性计划和信息提供论坛。

- 确定并开发在全行业适用的业务连续性计划和项目。
- 在证券行业和政府立法机构、管理机构和服务提供商三者之间建立联系，并提供通信和支持设备。

BCP 是一个不断发展的实体，SIA 会在网页上发布其最新信息。

[http://www.sia.com/business\\_continuity/html/background.html](http://www.sia.com/business_continuity/html/background.html).

这些工作要通过其 9 个分委员会实现。它们侧重于经济行业和特殊的业务连续性需求，而且每 6 个星期会在美国纽约和新泽西会晤。下面是其详细内容。

#### ①SIA BCP 指挥中心分委员会

这是一个战术性工作流需要建立的指挥中心。SIA BCP 会在出现严重灾难时启用。它将作为证券行业中心，负责事态通信和与响应相关的行业合作，并在灾难发生期间和发生之后在城市、州和联邦实体间建立联系。

SIA 指挥中心具有 24 小时昼夜会议线路，“钱包卡”包含了来自有关组织的联系信息和通知步骤。

中心确定了明确的工作流程、角色和责任。具体的通信协议则根据机构的不同而有所不同，如纽约市的 OEM 和其他城市机构以及州及联邦机构。

启用过程如下：

要求 SIA 成员在联合指挥中心中现实地聚在一起几乎不太可能，所以建立虚拟指挥中心实属必要。

当任何一位 SIA 成员公司检测到某事件发生或可能产生严重的行业影响时，SIA 指挥中心中负责联系工作的 SIAC 应急指挥中心（ECC）将发出通知。SIAC ECC 将尽可能多地从初期报告中获取信息，并发布一系列的预警通知。这些工作的摘要内容将同时公布在已有的安全网页上。

根据初期通知，SIAC ECC 应急服务管理层将召开一次会议，邀请受影响的成员公司、受影响的实体和必要的政府实体，并指定出一个由 5 人组成的评估小组。评估小组将决定是否需建立与城市-州应急事务运营中心联系，还是激活 SIA 虚拟指挥中心会议桥接线/或者向全体 SIA BCP 委员或更多行业内的联系人发出通知。

#### ②SIAC 应急事务指挥中心

SIAC ECC 负责分配电话号码，以用于 SIA 信息通信线路。电话 24 小时昼夜有人值守，服务在网桥两端都可获得。这样迅速的通信系统使用事先建立好的联系组名单，同时由一个具有 12 条线路的电话系统进行呼叫，发送电子邮件、传真和信息或确认收到通知。而且，ECC 的虚拟指挥中心会议网桥线路是一条标准的会议网桥线路，被 SIA 指挥中心包租。

##### a. 外部信息

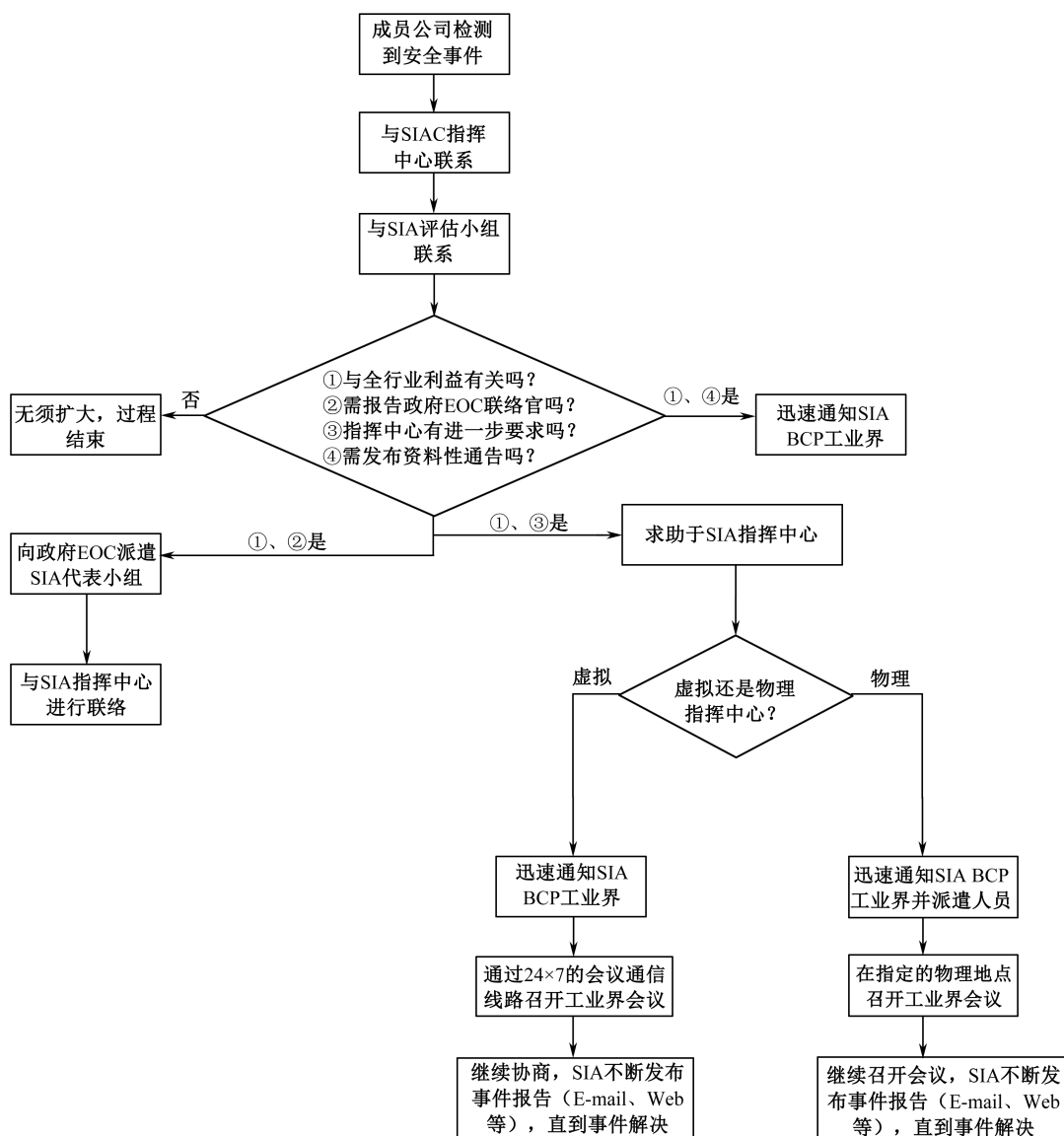
当某一政府实体或关键设备提供商意识到某种情况将会影响 SIA 成员的业务运行时，SIAC ECC 应急服务管理层将行使另一项功能，作为电子邮件联系点，向已有 SIA 成员重新发送信息。

SIA BCP 工作流程图如后图所示。

##### b. 交换和行业设备分委员会（DTCC，清算中心等）

提供交换和应用中连续性计划方面的信息。解释“我们防护什么”，将在成员公司团体的

协助下完成。建立满足行业业务连续性需求的基础性通用标准指南。此外，反映连接性和处理工作流程的计划也将在不同的行业组织中共享。



工作组还要为开发/提高已有计划提出建议，以满足大型金融中心提出的业务恢复需求。

#### c. 业务管理规划分委员会

侧重于（行业范围内的）特殊业务问题，负责为实体和固定收入产品领域开发灾难通信和问题解决协议。另外，也考虑操作、结算和清算等内部问题。在需要的情况下可以利用资产管理等其他业务。

#### d. 大技术管理计划分委员会

侧重（行业范围内的）技术问题，如企业恢复和为行业参与者制定协议并开发有关项目，以此确保业务顺利恢复。具体问题涉及塔楼、市场数据、贸易层技术、加密等。本分委员会的目

标是帮助行业 BCP/DR 测试建立一套长久的标准框架。

**e. 关键基础设施规划分委员会**

本分委会将侧重考虑与“生命线”提供商有关的问题。这些提供商包括电力、通信、供水、运输等关键行业的提供商（和应急管理机构）。必须制定与这些组织的合作协议，以确保能获得广泛的需求并实施灾难预防计划。

**f. 最佳实践措施分委员会**

致力于总结和传播“9·11”事件中汲取的教训。此外，BCP 将制定并提供关键管理和 IT 恢复最佳实践措施，并从已有实践措施中选取最好的措施，然后将其整合成最佳实践措施。SIA 2002 年 BCP 的调查问卷将由此工作组编撰并完成。

这项工作将主动与其他委员会进行合作。联邦储备银行和证券及交易委员会将制定出最佳的实践措施信息。

**g. 意识培养和教育分委员会**

为安全行业中的专业人士制定业务连续性计划领域的培训课程和材料。课程和材料主要侧重于制定和执行应急管理和灾难恢复计划这一安全行业内的最佳实践措施问题。本分委会将让不同的 SIA BCP 工作组参与到意识培养和教育中来。在制定了业务连续性计划的标准和最佳实践措施及指南后，会将它们统一整理到培训项目材料中，包括文章、演讲、会议材料和课程。这样的例子可见于 SIA 网页上的关键问题讨论区、SIA 和其他行业会议上的演讲材料以及 SIA 成员在应急情况下所提供的重要的应急信息。

**h. 商业区重新发展和未来需求分委员会**

要确保对金融社区关注，特别是关系到生命安全、安全性、灾难预防和业务应急等方面的问题，都要在世界贸易中心及其周边地区的重建中得到发展。这些问题是商业区成功重建的关键因素，对获得纽约城市金融社区长期的利润回报许诺来说必不可少。

**i. 保险需求分委员会**

由于世界贸易中心“9·11”袭击事件的影响，很多保险公司已表明，希望增加保险中的例外情况，最主要的是恐怖主义行为。某些保险金额（如业务中断、财产、员工债务、一般债务和人身等方面）也会大幅度增加。由于我们很难再在某些类型的保险金额上取得合理的赔率，因此这些行动将对我们的行业产生深远影响。

保险需求分委会的主要目的是总结灾难防御准则。那些能够证明自己由于遵守这些准则而降低了风险的组织将有权合理地要求降低保险金额。

**美国银行家协会（ABA）**

ABA 的金融隐私工具箱和盗窃标识通信工具套件可以帮助企业防止盗窃事件的发生，并向受害者提供帮助。保险公司也在向其业务和消费市场开发盗窃保险政策。

**C. 威胁**

由于自己暴露在全球各个领域的种种威胁之中，银行与金融部门的操作环境已经彻底改变。与公开共享数据网络的连接使这些机构面临威胁，这种威胁不受地域和时间的限制。另外，无论是否共享，机构资源与客户、提供商和合作网络的互联都将给机构带来间接风险，此时的金融机构没有办法直接评估或缓解这些风险。

威胁制造者有各式各样的动机来对机构或金融系统进行攻击。政治或种族原因也会引发攻

击行为，“9·11”事件就是很好的例子。在传统意义上而言，银行与金融部门所受的威胁一般来自犯罪事件和恶意事件。这些袭击事件可能是个人行为，也可能是犯罪集团的有组织、有预谋的袭击。多数威胁制造者的行为只是偷窃，但是，另一些威胁制造者的主要目的却是对设备进行破坏或使机构所提供的服务功能瘫痪。这类威胁也包括偶然行为在内，这种由部门内部或外部引起的威胁将造成金融损失并带来商业风险。

虚拟世界不仅为传统威胁的存在提供了新空间，也给其他威胁制造者提供了活动的机会，这有可能带来可怕的风险。虚拟世界中威胁制造者分为好奇人群、系统脆弱性搜索者、传统的犯罪事件或恶意事件的制造者，以及进行偶然行为的人群。好奇人群包括业余的破解技术爱好者。这些人使用别人开发的软件，不完全了解或根本不了解自己的行为带来的危害。系统脆弱性搜索者攻击系统的目的可能来自攻击成功后的喜悦或在同行中的技术成就感。犯罪事件或恶意事件的制造者，如恐怖主义者，制造威胁的目的与他们在现实生活中的目的一样，唯一的不同点就是在虚拟世界他们借助于网络空间。

从2000年和2001年的公开报道中可以看出，信息威胁使人们遭受了很多教训，也受到很多启示。2000年2月，美国多数电子商务网站瘫痪，造成约12亿美元损失。3月，两名英国青少年被捕，原因是他们攻击了5个国家的电子商务网站，并窃取了2.6万个信用卡账户。同年5月，菲律宾马尼拉某人发布了“爱虫”病毒。“爱虫”病毒迅速在世界范围内吞噬了多数公司的电子邮件系统，造成约百亿美元的损失。8月，两名哈萨克斯坦男子由于攻击纽约Bloomberg的L.P.计算机系统，企图盗窃20万美元而被逮捕。9月，大约1.57万西部联盟客户的信用卡和贷款信息被黑客窃取。在上述事件中，犯罪者都是通过执法部门的努力而被绳之以法的。

2001年里，网络空间的犯罪事件有增无减。黑客攻击了德克萨斯州的彩票网页，并在上面留下了一个鼓吹另一个操作系统优点的信息。一个被称为“skimmer”的家伙通过在零售机的信用卡终端植入恶意代码而窃取了信用卡账户，并将截获的账户发送出去。2001年7月和8月，“红色代码”感染了数以万计的服务器，其中很多属于金融部门。被感染的服务器将作为攻击美国白宫网站的跳板。幸运的是，由于得到了事先预警，白宫的技术人员及时更换了技术，从而避免了这一攻击事件。红色代码造成的损失估计为24亿美元。此类恶意代码可以迅速繁殖为大量变形体，这也是攻击类型的一种新型发展趋势。

随着越来越多网络空间攻击事件的成功，银行与金融部门应该和其他部门一起更好地为抵抗可能的破坏事件做准备，应认清其重要性。目前，即便出现了大量预警信息，并且有很多“矫正”办法，很多系统管理员也不能及时为保护系统做出响应。就“红色代码”病毒来说，尽管存在大量的预警信息和如何避免被攻击的办法，但是仍有大约100万台服务器受到感染。

无论威胁制造者的动机和形式是什么，其结果都会对机构造成威胁。金融部门应建立日常安全防范措施，具备一定的防护能力，以缓解普通攻击可能带来的威胁。风险评估过程能识别脆弱性、缺陷和金融漏洞，并能有助于制定行之有效的解决方案来转移或缓解风险。

不幸的是，各机构或部门整体面临的严重威胁并没有得到比一般威胁更多的重视。这是由于这些风险的发生概率比一般风险要小得多，对其进行防护的性价比并不高。所以即便是可能引起系统瘫痪等问题的高风险事件也不会受到重视。而此类事件将在相互合作的机构中产生级联效应。

最终，银行与金融部门用于解决威胁的保护办法并不能一致统一地抵抗来自敌对方的攻

击。例如，已有一些公认的方法可以在一定时期内抵抗瘫痪攻击，但这些措施在对付全局瘫痪攻击时则略显不足。

下表列举了公司中可能面临风险的资产、每种资产的风险类型、可用于抵抗风险的对策以及可使用的方法。对于这些风险问题的深入讨论和部门间的相互联系可参阅第 D 小节“摘要和总结”。

基本资产	风 险	对 策	可使用的方法
不动产和基础资产	<ul style="list-style-type: none"> <li>● 入侵；</li> <li>● 破坏；</li> <li>● 无法访问</li> </ul>	<ul style="list-style-type: none"> <li>● 周边防护；</li> <li>● 内部保护；</li> <li>● 网页备份；</li> <li>● 登录监视；</li> <li>● 警报系统；</li> <li>● 电力/设备备份</li> </ul>	<ul style="list-style-type: none"> <li>● 个体公司响应；</li> <li>● 地方当局的协调响应；</li> <li>● 合理的业务措施</li> </ul>
员工	<ul style="list-style-type: none"> <li>● 来自不满的员工的攻击；</li> <li>● 渗透活动；</li> <li>● 绑架/暗杀</li> </ul>	<ul style="list-style-type: none"> <li>● 加强对员工的监视；</li> <li>● 员工咨询；</li> <li>● 员工保护</li> </ul>	<ul style="list-style-type: none"> <li>● 个体公司的响应</li> </ul>
数据	<ul style="list-style-type: none"> <li>● 破坏；</li> <li>● 丧失完整性；</li> <li>● 盗取；</li> <li>● 操纵金融收入</li> </ul>	<ul style="list-style-type: none"> <li>● 数据备份；</li> <li>● 数据和防火墙的访问控制；</li> <li>● 审计踪迹/监督；</li> <li>● 加密；</li> <li>● 完整性控制</li> </ul>	<ul style="list-style-type: none"> <li>● 威胁报警；</li> <li>● 对较低等级异常现象的协调分析；</li> <li>● 协调响应；</li> <li>● 脆弱性报警和跟踪；</li> <li>● 合理的业务措施</li> </ul>
系统	<ul style="list-style-type: none"> <li>● 破坏；</li> <li>● 丧失完整性；</li> <li>● 对外包公司的依赖；</li> <li>● 丧失可用性</li> </ul>	<ul style="list-style-type: none"> <li>● 访问监视；</li> <li>● 周边防护；</li> <li>● 信息战的保护；</li> <li>● 入侵检测；</li> <li>● 应急/备份</li> </ul>	<ul style="list-style-type: none"> <li>● 威胁报警；</li> <li>● 协调响应；</li> <li>● 脆弱性报警和跟踪；</li> <li>● 合理的业务措施</li> </ul>
日常设备	<ul style="list-style-type: none"> <li>● 丧失可用性；</li> <li>● 渗透活动；</li> <li>● 破坏；</li> <li>● 操作</li> </ul>	<ul style="list-style-type: none"> <li>● 替换功能；</li> <li>● 内部能力；</li> <li>● 审计；</li> <li>● 第三方评估</li> </ul>	<ul style="list-style-type: none"> <li>● 威胁报警；</li> <li>● 协调响应；</li> <li>● 脆弱性报警和跟踪</li> </ul>
金融应急支持	<ul style="list-style-type: none"> <li>● 丧失可用性；</li> <li>● 破坏信息；</li> <li>● 破坏数据</li> </ul>	<ul style="list-style-type: none"> <li>● 多路径和精密线路；</li> <li>● 加密</li> </ul>	<ul style="list-style-type: none"> <li>● 个体公司的响应</li> </ul>

#### D. 摘要和总结

美国银行与金融部门负有保卫国家经济资产的责任。银行与金融部门在确保美国经济系统可信服务环境的同时，必须最大化地使用现有资源，以保障关键基础设施和基本资产。这是一项需要金融机构各行业以及专业化服务组织和服务提供商共同努力实现的任务。机构间的互依赖会使得基础设施复杂化，必须在保护这些设施的同时确保设施中分立组件之间的正常资金业务关系。并非所有的互依赖的强度都会得到处理，也并非所有的缺陷都得到识别及修改。因此，各公司和部门间的共同努力的目标就是了解和保护基础设施，当然除此之外还有很多其他工作要做。



为了向国家关键基础设施组件提供保护，银行与金融部门必须开发一份协调的解决方案来解决个体机构中的应急响应计划无法解决的问题。此外，部门应具有一定的灵活性——及时吸纳商业环境中具有重大影响的行业发展趋势和缓解风险因素的能力。这些趋势包括技术变更、全球化、行业内的合并等部门需要适应的行为。国家战略将提供指导设计、合作和实施部门工作的机制，以保护美国的金融系统。

银行与金融部门中的多数个体机构都制定了连续性计划，也执行了保卫资产的安全控制措施。总体上，对于识别威胁和脆弱性，银行与金融部门已具有足够的适应和响应能力。银行与金融部门正在努力执行第 63 号总统令的指示，即确定用于保护银行与金融部门关键基础设施的综合项目，以抵抗潜在的物理或网络空间威胁。与此同时，银行与金融部门还提交了一系列意向建议，用于响应基础设施面临的挑战。这些建议已经根据规章制度和指导方案得到了规范。同时，部门已决定以公共-私营联盟的形式继续与地方、各州和联邦的执法机构和政府实体进行合作。

除了为未来工作制定计划外，银行与金融部门已经起草了一系列保护本部门成员免受威胁影响的行动意向建议。部门间的协调员和行业代表来自不同的机构，他们组成的智囊团对部门的工作进行适当的指导，取得了一定成效。FS/ISAC 就是其中的一例，如第 1.B 小节所述，建立一个私营部门信息和分析中心来协助检测和刻画潜在的威胁和缺陷。

FS/ISAC 将继续强调安全事件和威胁所具有的全球性意义，提倡跨部门的信息共享。为此，FS/ISAC 及其他部门的工作将继续最大化地分配和应用 ISAC 的信息共享资源和 CERT 知识库等资源。

银行与金融部门的其他工作还包括 BITS 产品认证项目，详细内容见第 1.B 小节。结合其他行业协会，如美国银行家协会的宗旨，银行与金融部门提供了很多资源对信息传播和关键经济资产实施预先保护。

如国家战略中所言，银行与金融部门必须做好响应全球威胁环境中各式各样威胁的准备，无论这些威胁是来自于物理世界还是虚拟空间。这类威胁的范围很大，包括对物理基础设施破坏的恐怖主义事件，也包括威胁计算机服务提供商的虚拟网络空间站。其动机可能是政治上的，也可能是个人的；可能由个人引起，也可能由敌对团体发起。金融系统互联性的增强和信息的公开也是可访问性和脆弱性增加的原因。

2000 年和 2001 年发生了很多针对金融机构的网络攻击事件以及惨绝人寰的“9·11”事件。随着部门间合作的扩大，银行与金融部门必须采取协调一致的措施来保护关键基础设施。看似独立的攻击事件可能会具有级联效应，可引起系统瘫痪等一系列后果。

解决系统面临的威胁的一个办法就是跨部门的协作，包括检测、分析、传播信息和迅速响应。各机构的不能推卸自己需要承担的安全责任，但整个部门之中的相互协作则可实现安全系统和资源的共享，从而加强银行与金融部门对威胁的响应能力。

## 2. 关键基础设施保障战略指导

### A. 行动倡议

发生在 2001 年 9 月 11 日的惨剧已经使人们提高了警惕，人们已经意识到保护国家关键基

基础设施使其不受威胁的重要性。具体而言，该事件也使我们认识到金融系统的关键基础设施组件与网络空间内的组件同样需要关注和保障。银行与金融部门及时认清了形势，并在本战略的各项工作部署中表明了解决这一问题的决心。

尽管“9·11”事件是美国历史上最严重的恶性袭击事件，造成了最严重的经济损失，但它毕竟是很少发生的。但是，我们注意到网络空间内的信息攻击事件频率和强度在这几年已不断提升。所有迹象表明，类似事件将会不断发生，而且影响程度还会加重。这从2000年和2001年公开报道的事件中可以略见端倪。其中的很多还成为公众传媒和众人议论的焦点，包括“红色代码”蠕虫、美国在线信息系统的缺陷以及微软公司最新操作系统 Windows XP 中存在的问题。基于客户和市场的考虑，多数公司不愿公开其对抗信息犯罪、计算机病毒和其他技术缺陷的措施。这是在处理有关计算机事件的公开信息时必须考虑的。

现在已经到了政府和私营机构采取其他行动来保护关键基础设施的时候了，人们不得不面对来自网络空间的潜在威胁。确实，网络空间攻击会造成严重损失，浪费巨大金钱，并破坏一个组织的声誉，但并不会在物质上影响金融部门的持续运行和服务。金融部门应未雨绸缪，在灾难来临之前制定出正确的挽救措施，必须知道正确的业务工作措施，建立并执行切实且行之有效的政策。

## B. 原则

### 指导原则

银行与金融部门建立了用于保护国家关键基础设施的四项指导原则：

- 必须对银行与金融部门的核心基础设施进行检查，以确定和评估其面临系统化风险的领域和暴露点。
- 通过使用合理的风险管理、业务和安全措施，核心基础设施的所有人和管理者必须参与基础设施协调运行的保障工作。
- 核心基础设施的所有人和管理人必须积极的相互保护的协作，必要时要以合作的方式抵抗系统化风险。
- 必要时，联邦政府要联合核心基础设施的所有者和运营者，对业内和业外的基础设施进行保护和积极响应。

### 前提

以上原则的几个重要前提是：

- 公共-私营联盟是迎接新型和非传统技术挑战的重要保证。
- 需要改变和修正政府在20世纪以来对行业合作的管理政策框架和态度，以此帮助确立和保持这种合作联盟。
- 公共部门和私营部门都必须对安全支持和业务利益进行权衡。

## C. 框架

### 准备和防范

由于银行与金融部门长期对有形和无形资产的监护，它已确立了良好的公众形象，赢得了客户信任。保持公众信任是金融部门一直以来的主要目标。为了实现这一目标，部门成员需要

进行跨机构的工作，以制定安全地保卫客户信息和资产的指导政策和标准。这一任务的重点在于为机构和行业建立防止其待保护的资产受到非授权访问或操纵的政策，特别是流程和技术框架。本部门通过下述工作提供了典范：

- 制定强有力的政策和流程，并就这些政策和流程进行交流与巩固，以对客户和内部交易过程进行管理和保护。
- 通过内部员工和外部审计与咨询公司，建立定期自评估和审计工作。
- 采用领先的安全技术，如加密、特殊的硬件和软件。
- 使用强有力的安全保护措施保护机构间的交易活动，如资金转账、清算和结算等敏感的交易活动。涉及的机构包括诸如国际银行间金融交易协会（SWIFT）等各类清算和储蓄协会。
- 开发安全技术标准，在国家和国际标准机构的帮助下管理金融交易过程。这样的机构包括美国国家标准学会（ANSI）、国际标准化组织（ISO）和认可标准 X9 委员会。
- 在行业协会的协助下，联合开发和共享领先的安全和保护措施。这样的协会有美国银行家协会（ABA）、BITS、美国独立社区银行家协会（ICBA）和证券工业协会（SIA）。

#### （1）本行业在准备和防范工作中的态势

对银行与金融业的研究表明，银行与金融部门最好在个体公司一级就做好防范网络空间和基础设施威胁的准备。这样可以更好地树立公众对金融系统安全性和可靠性的信心，有助于取得持续的成功。除了联邦和各州长久以来对各类大型金融机构（如保险委托人、股票经纪人和发行人）发布的法规之外，银行与金融部门也已经在保护其资产方面取得了显著成就。到目前为止，银行与金融部门已采取了很多防范措施来解决传统的内部或外部诈骗、服务瘫痪和丧失运行能力等问题。对于这些威胁，可以从公共机构的角度认识它们，也可以从系统化风险角度理解它们。

金融部门有能力响应系统化风险，“千年虫”问题就是个很好的例子。本部门采取了事先的预防措施来对日期变更可能引起的失效问题进行了调整，从而避免了计算机故障而引起的破坏。金融业对“千年虫”问题的解决具有一定的深度和广度，这也为解决系统瘫痪等其他问题提供了解决的模板，如网络空间内的金融服务业攻击对美国经济造成的打击。银行与金融机构很多现行的防御措施在此方面具有很好的功能，但从国家安全角度看，需要有一个更有力、协作性更强的响应措施。这需要本部门内的预防和抵抗能力的加强，这样的办法将确保并提高信息共享的力度、安全保障、合理的实践措施以及脆弱性评估等。

#### （2）信息共享

金融服务领域从事信息安全工作的机构在几年前就联合了起来，共享了威胁信息，推动了合理措施的出台，并协调了行业内的活动。行业协会的出现是对诸如纽约清算中心安全委员会等正式机构的有力补充。目前最有影响的是 FS/ISAC，如第 1.D 小节所述。为了解决国家基础设施经济结构的问题，在不违反反托拉斯法的原则下，要保障和加强这类合作。

#### （3）保障

行业内的独立公司很多都是独立采取保障措施的。国家标准与技术研究院（NIST）通常是独立评估和安全产品和解决方案的有力补充，但是保障共享工作却仍处于“内部”阶段。在参与信息保护技术标准定义的成员中，金融证券业的安全专家是积极的因素。这些成员有美国国家标准学会（ANSI）、国际标准化组织（ISO）和 X9 标准委员会，ABA 在其中充当了

秘书长的角色，ANSI 认可标准 X9 委员会去制定和发布金融服务行业的建议性技术标准。与提供商和学术专家的合作结果是得到了提供商认可和保障的基线。BITS 产品认证项目及其电子商务产品和服务安全轮廓的建立和执行则提供了一种新型的保障措施模型，应在部门成员间大力提倡。

#### （4）最佳实践措施

在安全政策、流程和政策领域的工作就是不断地确定、编辑、讨论并总结出一套综合的最佳实践措施。在保护客户信息、敏感交易过程和数据时，金融基础设施的核心服务商必须坚持执行最严格的实践措施。本文第 3 章描述的 BITS 自愿指南和最小业务实践系列、ABA 的金融隐私工具箱和盗窃标识通信工具套件、内部审计师协会（IIA）出版的指南和标准、信息系统审计与控制协会（ISACA）以及信息安全论坛都是这方面的主要范例。

**部门行动：**在行业和专业协会的帮助下，银行与金融部门将继续开发、提炼和总结出“最佳实践措施”。

**部门行动：**银行与金融部门将鼓励使用通过检测的产品，以改善产品安全性能。

#### （5）评估

对国家关键基础设施的保护包括对攻击的预先防范措施和遭受攻击后重建关键基础设施的能力。这两方面都需要确定出核心基础设施的关键功能和服务内容。而且，基础设施的关键组件必须能够经常接受严格检验，并对它们的状态和实践措施进行评估。本部门推荐了以下的不同方法以供参考：

- 机构对内部控制环境的自我评估及实践工作的定期自我评估。
- 可信第三方对核心机构和过程的外部评估和审计。
- 对本行业中关键业务内的交易流、过程和流程进行正式的分析和评估。这需要银行与金融部门的领导以及可信第三方的支持。
- 跨行业间的相互评估对象包括银行与金融部门所依赖的关键基础设施组件，如通信设备和能源。

虽然评估是对某些方面及时的统计反映，但是新型的脆弱性、威胁、风险和对策还将不断涌现和进化。出于行之有效的目的，脆弱性、风险及其他评估方法必须根据需要及时迅速地升级。迅速地反馈评估结果具有很重要的意义。通常，一个完整全面的部门评估工作是一项不可能在短期内完成的艰巨任务。因此，为了完成一项全面的评估工作，需要有一套方法对任务的执行进行指导。

第 1.C 小节中概述了金融服务部门所面临的威胁。其中的威胁主要针对的是可能给金融机构的关键服务提供机制造成破坏的系统化风险。然而，对损害客户信任基础的威胁也要给予足够的重视。20 世纪以来，金融服务部门一直在致力于建立客户的信任，同时通过这种信任关系以更为有效且价格低廉的方式来支撑新式的服务。广义上讲，客户的信任和信心是建立在金融部门保护客户信息保密性、完整性和可用性能力的基础上的。任何对这种能力的严重威胁都将破坏客户信心的建立。

对盗窃的标识是一个必须考虑的风险内容。对个人信息的盗窃可以通过各种方式实现，而且这种风险也不仅限于银行与金融部门。目前，很多实体都有收集客户个人及其经济信息的习惯，因此这些信息受到了多方面的威胁。无论威胁来自哪方面，银行与金融部门都必须保证信息的损坏不会导致对经济收入信息的盗用。例如，金融部门可以在进行信用卡交易前建立验证

和鉴别程序。类似地，金融部门要创立阻止以职业托词获取个人信息的方法，减少这种行为的可能性。

可确保工作持续运行的连续性计划是否有效也是面临的一个风险。很多机构都采用了连续性计划来解决由物理和自然威胁引起的业务风险。即使是很短时间的运行中断，如果再次发生，也会使客户丧失信心，所以金融机构必须确保核心服务和过程具有最大程度的可用性。必须使设备有一定的冗余度且能经常运行，这样才能限制物理和自然威胁的升级。例如，金融机构必须考虑其通信服务提供商、能源和用水，确保提供商的多样化，以确保任何问题都不会对部门服务的可用性造成太大损害。

### 检测和响应

#### （1）目标

检测和响应银行与金融部门信息基础设施面临的威胁是一项重要的工作，本部分内容为定义其框架提供了指导、总体概念和战略。这部分的目标是在短期内迅速制定出事件管理政策，包括在大范围内威胁金融服务交付的事件和对国家安全或日常经济运行能力存在威胁的事件。我们不拟解决国家范围内的问题，除非若因某个关键问题可能会引起一系列对整个金融部门的多数机构造成危害的事件。

银行与金融部门正通过不同的防护机制来减少其遭受攻击的可能性，逐步地缓解风险，如脆弱性评估工作、周边安全防火墙和入侵检测系统的使用。内部防护机制还有访问控制系统和制定安全标准及合理的保护措施。然而，由于所面临威胁的多样性和不可预知性，所以不可能确保能防御所有的攻击。同样，无论是个人还是团体，对铁了心的攻击者的威慑也不可能永远都取得成效。我们必须做最坏的打算。

理想的检测和响应计划的目标是自动地识别出攻击行为，并自动进行响应。虽然金融服务机构所应用的入侵检测系统在不断更新和改进，但仍处于初期阶段，不能提供一个完全自动化的响应功能。另外，不是所有的设施都能受到入侵检测系统这把大伞的保护。事件发生的原因多种多样，可能是蓄意的，也可能是无意的；范围可能集中，也可能很分散；攻击可能是直接的，也可能是间接的；可以是网络空间内的，也可以是现实世界中的。无论采用何种机制，也无论事件发生的动机是什么，对关键基础设施的保护必须解决金融服务的恢复问题。

#### （2）金融部门防御工作的战略特征

必须认识到，我们无法预测所有的事件，必须牢记应该通过合作来进行事件响应。本战略框架的目的就是协助执行一套适用于关键的管理和恢复的工作步骤。其中包括以下内容。

##### ①早期识别和信息共享

一项重要的任务就是对可能威胁金融服务的大规模事件进行早期识别。通常安全事件会以各种形式呈现，因此在初期检测和识别时很难确定他们真实的影响范围。刚开始进行识别工作时，组织应该对自身遭遇了系统或网络瘫痪的假设进行响应，因为在很多时候，当组织最终才将某事件归为安全问题时，已经浪费了很多时间。共享 FS/ISAC 提供的信息对理解事件影响的范围是非常必要的。事件分析可以有助于判断问题的属性，有助于确定是否存在潜在的系统故障。

部门行动：银行与金融部门要鼓励 FS/ISAC 所有层次上的金融机构成员，这样有助于及时进行缺陷和威胁影响信息的交流，同时可以完善现有成员提交的事件报告。FS/ISAC、BITS 和

ABA 等协会应提出建议，以加强合作。

## ②快速分类

一旦确定某事件可能与安全问题有关，就必须及时对其进行评估和正确的分类，以使行业成员能够迅速了解事件，适当做出响应。国家政策主要解决的是可能在大范围内严重威胁金融服务提供和完整性的事件。希望所有组织都建立连续性计划，以解决会影响金融服务提供的局部问题。

部门行动：银行与金融部门已经制定了一套正式的且结构化的事件分类流程，以帮助部门成员及时发现可能导致系统故障的严重事件。

## ③事件升级

一旦某事件被定性和分类为可能影响关键基础设施的事件，各级组织便需要有一种汇报的流程和通信结构，将事件报告给本部门和国家机关。通信设备必须有一定的冗余性，以确保在主设备丢失或被破坏时可以继续提供服务。必须有一个能够考虑到所有信息源的评估程序，并能在恰当的时候宣布出现“国家危机”。

部门行动：银行与金融部门将制定灵活的汇报流程和通信协议，用于事件的通告和升级。

## ④动员

当宣布了国家危机后，必须迅速组织应急小组，并派遣成员对事件进行管理。事件管理包括保存、功能恢复和恢复。我们希望各机构已经建立了其自身的危机管理过程，并为问题解决分配了一定资源。内部职员应得到专业技术和知识等外部资源的支持。

部门行动：银行与金融部门将制定一个对事件进行快速评估和集中化管理的流程，用于事件管理中专业技能资源的标识。

## ⑤重建和恢复

当有不止一个基础设施时，一个事件会影响有相互关联的基础设施，因此重建管理非常重要。由于事件有其各自的特殊性，因此在事先设计方案时应优先考虑对基础设施组件进行恢复。应逐步舍弃在处理紧急事件时所采用的临时解决办法。在危机解除后，专家应回到各自的工作岗位上。而且涉及的所有团体都应该参与事件的后续分析工作，为添加保护和预防措施献策献力，目的是避免类似事件再次发生。管理小组还要检查被更改了的事物，并将这些内容写入应急响应计划，以弥补不足，纠正问题。恢复工作应有秩序、有计划地进行。

银行与金融部门的计划里还要检查出那些单个机构无法完成，而必须要靠整个部门共同努力才能解决的严重业务设施故障。这些设施也许并不在机构内部，如 FEDWire 和通信设施。还要同时考虑组织间的金融合作，并在某些组织无法完成其金融责任时，使用不同的风险管理模型来决定其资金处理的需求。在一场大灾难过后，行业部门和对应的政府机构应对其中发现的问题进行讨论，并建立和完善恢复和重建计划。

部门行动：银行与金融部门将建立一套关键基础设施的恢复计划和流程。

## ⑥测试

为确保可持续发展，必须使用多种场景对计划进行定期测试，以确保其能继续应用，其中应涉及所有可能参与事件响应的机构。对测试结果进行评估后，很可能导致对计划进行修改，修改后的计划还将接受进一步的测试。这种测试和修改的循环过程是为了保持计划的灵活性和应用性，以适应不断变化的技术、威胁类型、缺陷和部门合作内容。

部门行动：银行与金融部门将制定出能定期测试和评估响应能力的计划。

#### D. 总结和结论

银行与金融部门已经意识到保护美国国家基础设施物理设备这一安全工作的重要性，希望通过执行此战略中提出的活动来解决物理问题。与此同时，银行与金融部门也认识到网络空间威胁事件发生频率也在上升，摆在金融系统和客户信息前面的危机也越来越大。金融部门在以往监护有形和无形资产时一向口碑很好，保持客户的公众信誉一直是本部门传统上的主要目标。银行与金融部门为保持对客户的信誉和领导国家关键基础设施的保护工作，已经制定了四项基本原则：

- 银行与金融部门必须对核心基础设施进行检查，以确定并评估暴露在系统化风险中的领域。
- 通过采用合理的风险管理措施、业务措施和安全措施，核心基础设施的所有者和运营者必须参与基础设施保障工作，并达成一定共识。
- 核心基础设施的所有者和运营者应该积极地提供相互保护，并在必要时以合作地方式面对系统化风险。
- 在必要时，联邦政府应该与这些所有者和运营者合作，对行业内部和行业外部面临的系统威胁进行防护和响应。

银行与金融部门应该实行机构间的跨机构合作，制定出保护金融资产的机制和方法，以确保自身信誉。为了防止非授权访问和非授权使用行业内部的资产，部门的工作重点应该放在政策、流程和机构技术框架的建立上。其中包括准备安全工作指南和标准，并对客户信息和资产提供保护。总体上，银行与金融部门应比其他部门更好地在个体公司级上下功夫，以确保网络空间和其他基础设施不受到威胁。

单个公司的努力并不能完全消除系统威胁。因此，部门成员还应该整体联合起来，一起努力去确定、评估和解决威胁。“千年虫”问题的解决具有很好的广度和深度，为其他系统故障的解决提供了一个榜样。如果没有细致的计划和指导方案，联合响应工作是不能够满足规定的要求的。在解决国家基础设施经济构架中存在的威胁问题时，必须确保并加强这样的合作，但也不能违反反托拉斯法。

为了使威胁识别工作更有成效，还要进行编辑、讨论、编写等工作，直到完全编写出一套有关安全政策、流程和技术的最佳实践措施手册。银行与金融部门还要借鉴行业协会和专业协会的经验，继续开发、提炼并总结出“最佳的实践措施”。另外，保障措施也是威胁识别工作中的重要内容之一。大多数单个公司在进行安全保障工作时，一般都各行其是，而在最近的保障工作中很多公司已经展开了合作。BITS 产品认证项目最新的研究成果为安全保障工作提供了新的样板，应鼓励部门成员使用。通过合作，可以共享资源，以达到从单个公司到整个部门中均能改善其安全实践的目的。

国家关键基础设施的保护工作包括两部分，一是之前的预防措施，二是之后的重建工作。这要求对关键组件、功能和服务的维护，并保障对安全状态和措施进行经常的严格检查和评估。技术方面的工作包括机构内的自评估、外部第三方对核心基础设施的评估和审计、对行业范围内交易流的评估和分析以及跨部门的相互评估。评估中使用的方法必须能确保有一定的目的性，能为制定长期综合评估过程及时提供信息。

对关键服务的交付机制造成的破坏威胁到了客户对银行与金融部门的信心。为了确保客户

信息的保密性、完整性和可用性，银行与金融部门必须采用有效的事件管理过程。在管理复杂事务时，部门间的合作是解决系统问题的关键，这样才会使事件处理获得成功。银行与金融部门应为危机管理、恢复工作制定一套工作计划。

对有可能会在大范围内威胁金融服务角度机制的威胁要做到早期识别。对单个事件进行分析后，通过事件的模式便有可能发现该事件可能引发的系统故障。金融部门应鼓励本部门 ISAC 的成员进行早期识别工作，一旦识别出事件，并对其有了一定理解，就应正确地对其进行评估，并正确分类，这样可以有助于迅速通知和响应。金融部门还应该有一套完整的结构化的分类过程，这有助于及时发现系统故障。在了解了事件情况并正确分类后，还需要制定出报告流程以及通信体系，以使本部门和国家机关了结事件的过程。

如果某事件可能影响多数相关的基础设施，那么重建的管理工作是非常必要的。在这些事件中，银行与金融部门必须开发一套用于关键基础设施恢复工作的计划和方法。本部门应该与公共机构和私营团体一起，开发并使用事件管理系统来进行危机管理工作。在重建管理计划将定义一套可以迅速建立的指挥和控制结构，还要定义关键资源的标识和部署过程，从而有利于对事件的快速评估和集中化管理。金融部门应该制定计划来定期检测和评估这些过程，以确保其在解决美国基础设施威胁时的时效性。

### 3. 加强基石建设

银行与金融部门在防御网络空间和其他威胁时已经取得了令人瞩目的成绩。本部门未来的安全工作需要将评估、管理过程开发、教育、推广、研发等关键工作有机地协调起来，以确保国家金融服务基础设施的完整性。

#### A. 部门评估工作

基础设施保障工作的一项中心原则就是依赖于对本部门现状的正确评估。“必须对银行与金融部门的核心基础设施进行检查，以确定存在风险的领域，并对其进行评估。”部门的参与者有以下各种方式来协助完成这一目标：

- 在财政部门的支持下，对存在暴露的领域进行标识和评估，并评估有可能给本部门带来风险的互依赖性。
- 每半年对基础设施进行一次检查，根据技术更新的情况标识最新的缺陷和风险。

评估对本行业的模型和仿真过程进行开发和实施的可行性，以评估和解决核心基础设施面临的系统化威胁。

#### B. 部门协调和管理过程的制定

公共-私营部门日常处理的很多情况都会影响到关键基础设施，并因此而最终会影响到其服务的可用性。一般而言，这些情况由基础设施组件的所有者和运营者负责处理。基础设施的强健性和多样性、冗余性及应急计划均能确保服务的快速恢复。

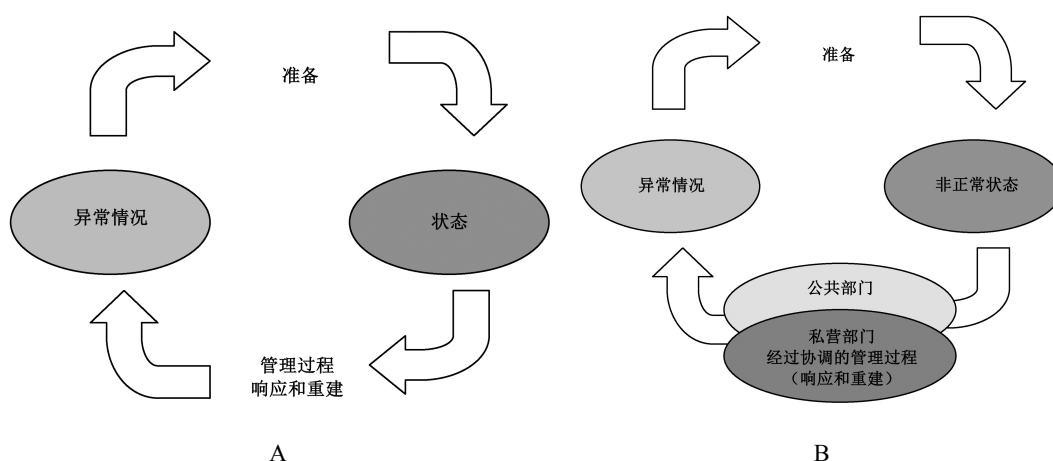
部门服务的可靠交付理念中始终贯穿的一个国家目标，就是对一些超出银行与金融部门正常管理能力范围的事件的关注，如“9·11”袭击事件对纽约和华盛顿地区的国家基础设施造成的破坏。因此，谨慎地对类似情况进行准备和筹划可以确保政府和私营部门能够进行整体的



协调响应。

下面两幅图说明了上述情况。图 A 描述的是常规的基础设施事件准备过程，如对自然灾害、能源短缺、通信中断或物理设备破坏的防范等。图 A 介绍了常规的恢复过程。日常“管理过程”足以确保这些服务的重建工作，使其恢复到原有状态。从这类情况中总结的经验具有反馈作用，根据这些经验可以对准备阶段的工作进行进一步修改。

国家战略中的基础设施保护工作将解决一些特殊的威胁问题，通常称为“结构化威胁”，这是一般日常业务运行不能解决的情况。在这种情况下，公共-私营部门必须协调管理过程，使关键基础设施服务恢复到正常状态。如图 B 所示，在解决异常情况时，“协调管理”是一个必要的过程。协调管理过程的另一项关键是战备工作以及对结构化威胁情况的检测。由于对结构化威胁影响情况的识别是至关重要的，所以部门间的有效且稳定的信息交换过程是相当关键的。



银行与金融部门应该制定出正确的战备等级，并始终起到领导作用。在与关键基础设施安全合作组织（PCIS）的合作下，银行与金融部门将从其他部门和组织寻求支持，因为这些部门在准备和协调管理响应过程上是很有经验的。有了来自银行与金融部门的运行人员及公共部门的支持，目前的工作将持续到 2002 年年底。

**部门行动：**银行与金融部门要鼓励 PCIS 的参与者和某些政府实体制定“协调管理过程”（CMP），它将在需要公共-私营联盟来协调响应某些问题时起到积极作用。这项工作包括“基础设施条件等级”（INFRACON），目前由 FS/ISAC 负责制定，并将映射到国土安全咨询系统和规划中的一些响应制度中。初步的 CMP 将在 2002 年内完成。

**部门行动：**银行与金融部门将制定用于对系统攻击进行分类的方法，并建立正确响应的工作框架。

**部门行动：**一旦确定了正确的响应过程，银行与金融部门将利用场景测试来对响应过程的完整性和及时性进行常规检验。

### 各机构的角色和责任

金融机构应把安全事件管理工作整合到整体的关键事务管理工作计划中去。其中包括确定与其他机构，如 FS/ISAC 和地方立法机构的重要合作。计划中还要包括事件响应工作的具体条例、对第三方团体的通知、对关键响应资源的确定以及事件调查过程和文件要求。同时，还必

须考虑应急操作和恢复。

各机构的责任包括以下内容：

- 执行最初的事件检测、分析和分类工作；
- 向 FS/ISAC 及其他必要的数据库进行事件汇报，随时更新汇报的内容；
- 启动事件遏制和响应计划；
- 在恰当时对事件升级；
- 执行应急和恢复计划；
- 与地方当局的工作相协调；
- 根据相互协作协议，与其他相关服务机构进行工作协调。

#### 需要进一步定义和分配的行动

由于 FS/ISAC 与其他 ISAC 的特殊关系，它是银行与金融部门间协调工作的关键。

### C. 教育和推广

银行与金融部门只有对行业领导人、管理者、操作者和其他利益人员进行教育和推广，才能得到他们对新政策的支持。关键基础设施保护总统委员会已经意识到，关键基础设施保障的有效教育和推广应该是各部门必须的内容。根据委员会的指示，提高全民对基础设施威胁、脆弱性和互依赖性保障问题的认识是非常重要的，这只有通过教育等其他正确的工作来实现。特别的，还要提高基础设施所有者和运营者、企业的基础设施用户、联邦和各州高级政府官员及一般大众的意识。

在银行与金融部门内部，教育和推广到目前为止主要指的是让部门信息安全专家重视第 63 号总统令所阐述的目标。需要向以下成员传达部门工作的精神：

- 政府的执法、立法机构；
- 金融行业的 CEO 和 CIO；
- 其他经济部门；
- 国际领域。

另外，银行与金融部门还应该做到：

- 召开年度和年中会议；
- 在国会召开前收集资料；
- 向联邦机构汇报；
- 在行业 CEO 和 CIO 的集体大会上报告；
- 在信息安全和金融会议上报告；
- 参加有关关键基础设施的国际双边会议；
- 支持 PCIS 的工作；
- 积极招募 FS/ISAC 成员。

参考附录 B（略），可以了解工作的部分列表。

在部门工作取得成功的同时，还要有一个更加综合和系统化的教育和推广的纲领，建议如下。

#### 教育和推广工作的目标

教育和推广工作的基本目标是为完成银行与金融部门关键基础设施的任务提供强有力的

基础。这种支持来自于银行与金融部门中各利益团体对如下工作的参与和付出：

- 核心基础设施的战略保障目标；
- 推动基础设施保障工作所需的措施的实现（如战术目标，包括信息共享、合理的安全实践措施、员工培训、跨国合作以及参与系统事件的响应协调管理协议的制定）。

银行与金融部门已经或着手制定不同的战略、战术计划。部门的教育和推广工作应该提高人们的安全意识，加大影响力，加强人们的参与力度：

- 对核心基础设施基本组件的标识和风险评估；
- 为核心基础设施保障工作制定和吸纳合理的实践措施；
- 扩大 FS/ISAC 的成员范围和信息发布广度；
- 使用通过 BITS 或 NIAP 测试的产品；
- 对保护关键信息基础设施工作的立法；
- 跨部门的关键基础设施信息交换；
- 建立公共-私营部门协调响应的管理过程；
- 跨国合作和协作；
- 对高产出研究和开发建议的制定；
- 加强对员工的信息安全培训；
- 采用合理的行业业务实践措施。

### 信息传播和方法论

银行与金融部门将与财政部门合作，共同制定出教育和推广的项目。根据优先等级定义，通过将教育和推广工作的重点设在公共部门官员以及基础设施所有者和运营者的范围内，将更容易实现上面提到的战略和战术目标。银行与金融部门的基础设施安全工作是一个必要的共同体。基础设施安全的综合提高会使金融系统的所有用户受益，包括客户和一般大众。当然，在有可能时，银行与金融部门将利用其他机构，如 PCIS、联邦各部局和贸易协会组织的信息安全意识培训活动，在一般大众或目标对象中产生影响。

### 基础设施的所有者和运营者

银行与金融部门的机构中，最主要的人员对象是 CEO、CIO、CTO、CISO、CSO、委员会主席以及不同委员会的委员，如审计委员会、金融委员会和投资委员会。其他对象也对整体政策和业务实践有一定影响力，如立法者和规范制定者、投资人、保险人、内部和外部审计师、贸易协会、产品和服务提供商、咨询公司以及主要客户。除了必须强调的国家安全和系统化的风险管理这两个主题外，提倡在公司一级实现基础设施保障的有效业务案例也是一项工作重点。大多数情况下，业务案例可以根据风险对数据保密性、完整性和可用性的影响来定义，这是影响金融机构与其客户之间信托关系的基础，而且这些风险也会产生一些经济上和法律上的后果。

财政部与银行与金融部门已将主要工作对象确定为部门的信息安全官员，并取得了显著的成效。由于以信息安全官员为主的听众群体具备足够的知识和能力，因此就成为了教育和推广工作最关键的对象。尽管如此，银行与金融部门为核心基础设施制定的战略目标仍需要有更广阔的听众基础。

## 基础设施所有者和运营者的行动计划

基础设施的所有者和运营者还要确保以下行动的实施。

部门行动：继续支持财政部举行的年度会议，会议成员包括银行与金融部门协调委员会的成员以及曾参加了 1998 年、1999 年和 2000 年会议的人士。银行与金融部门应就今后几年的会议制定时间表，注明会议召开的大致时间和议程。

部门行动：银行与金融部门将制定并传达合理的关键基础设施保障措施，使不同层次的所有者/运营者能够采取保障措施，或要求其所在组织改善基础设施保障工作。这项工作还包括编写一本合理的保障措施手册。

部门行动：银行与金融部门将与财政部长一起召集有行业内的总裁和高级政府及法律官员参加的会议。可以向高级金融工业界的官员递送区域关键基础设施保障工作的简报（由区域公共机构的官员主持）来支持这项工作。

部门行动：银行与金融部门组成的行业协会将在会议、论坛和讨论会上向 CEO、CIO、CTO 等高级执行人员汇报存在的问题。这样的协会包括（不仅限于）ACORD、美国银行家协会、美国社区银行家协会、银行管理局、BITS、金融服务圆桌会议、美国独立社区银行家协会以及证券工业协会。

## 公共部门

公共部门中的主要对象包括联邦、各州和地方的管理部门、立法部门和执法部门以及与部门业务活动有关的贸易协会等组织。银行与金融部门已经为公共部门制定了有效且高效的文件，其内容已记录在写在财政部 2001 年 3 月发布的政策和基础文档中。这些文档中记述了部门整体的关键基础设施项目，强调了对国家任务的响应，强调了公共-私营部门合作的重要性，强调了系统化风险的严重性，强调了核心基础设施各自的目标，强调了银行与金融部门起草国家计划时应该注意体现的精神。特别是，根据第 63 号总统令下达的主要任务，银行与金融部门已经下决心要取得实质性的进展，FS/ISAC 便是一个重要的例子。

银行与金融部门建议采纳以下工作。

部门行动：在与财政部合作的前提下，银行与金融部门将根据 2001 年 3 月提出的模型，向公共部门的官员进行汇报。汇报对象包括联邦各部局、国会的关键成员和国会职员、国家组织和协会、贸易协会。

部门行动：银行与金融部门将制定行动清单，列出每个对象在协助本部门完成 CIP 任务时需要采取的行动。

部门行动：银行与金融部门将统一印制和发行材料文档。这些材料将被提供给本部门的代表，以便与公共组织进行交流，或者应用于更多的场合，如会议、媒体等。文档材料将包括 PowerPoint 表格、论题和演讲或文章示例。

部门行动：银行与金融部门将制定部门管理人员的名单，根据上述标准化材料，这些人将被安排进行演讲、访问、汇报或出席部门 CIP 项目的媒体见面会。本部门还要为今后的贸易协会、行业、公共部门对应的相关活动制定出优先顺序表，以便通过部门协会动员群众参与。

有关这些项目的必要资源，参考附录 B（略）。

### 理想结果和绩效评估标准

为了评估教育和推广工作的有效性，有必要预先设定理想的结果，对其进行优先级排序，并建立绩效评估标准。绩效评估标准的制定必须对每个理想结果量体裁衣，必须确保其合理性，确保资源的有效且高效的分配。理想的结果包括部门协调委员会在工作中的不断参与、对部门风险评估工作的广泛支持和期望以及 FS/ISAC 的成员的增多。

### D. 研究和开发

研究和开发是银行与金融部门内的一项特殊领域，因为与其他部门（如能源部门）相比，银行与金融部门没有政府的资金支持。

部门行动：银行与金融部门将参考政府的研究建议和开发提案，并为部门优先领域提供反馈。

### E. 总结和结论

银行与金融部门认识到，要保护美国金融系统下属的关键基础设施组件不受破坏，其工作很复杂。在开发协调管理部门的响应管理计划时，要确定和评估基础设施面临的威胁。本部门内的很多机构已经采用了大量安全项目和连续性计划来处理日常业务运行中面临的“一般级”威胁。这些管理过程已经足以确保服务重建和运行恢复正常。本部门建议各金融机构在制定关键事务管理计划中嵌入安全事务管理的内容。

然而，银行与金融部门面临的威胁所带来的影响可能会超出单一机构。国家战略中提到的基础设施保护工作就是为了对付这类特殊情况，“结构化”威胁不可能由日常运行解决。为了对这类威胁进行防御，本部门建议采纳一系列内部和外部的协调工作和提案，以增加部门成员对安全方案的选择余地。协调公共部门与私营部门间的管理工作对于将关键基础设施恢复到“正常”状态非常必要。

协调管理过程的关键是“准备”工作，它有助于银行与金融部门了解和评估威胁环境。银行与金融部门将正确分配准备工作，并自始至终起到领导作用。本部门与 PCIS 均需要来自其他部门和组织的支持，因为这些部门和组织具有准备和协调管理响应过程这方面的经验。银行与金融部门还要推出对系统攻击进行分类的方法，并为正确的响应建立框架。一旦建立了响应过程，银行与金融部门将使用场景测试，对响应过程的完整性和及时性进行常规检验。

本部门内事件响应的一个重要内容，是建立事件指挥系统（ICS），对需要多个机构一起响应的事件进行管理。要管理能影响多个机构的事件便需要对各类资源和能力的协调。一旦多个机构参与其中，就必须迅速建立起指挥结构，这样才能高效地使用资源，以便高效地管理事件，实施恢复和恢复工作，并开始重建工作。指挥结构必须具有足够的灵活性，以能够容纳任何数目的机构，并能在事件恢复到正常状态后自动解散。此结构要求制定任务内容并设立目标，并根据战略和战术计划的具体要求来完成任务。在向所有团体传达有关状态、临时结果和有效的事件响应方法时，ICS 是非常有用的。ICS 的结构可能包括的元素有指挥、计划、后勤和操作，以便协调整体部门对威胁和事件的响应工作。

对银行与金融部门的行业领导人、管理者和相关利益方的教育和推广直接关系到是否可以得到更多地对新活动的支持。其他必要的工作还有与政府机构的管理部门和立法部门、金融部门、国际组织等进行沟通。虽然到目前为止银行与金融部门的工作取得了一定的成绩，但是仍需要进行更为综合和系统化的教育和推广项目。这项工作的基本目的就是关键金融服务系统

的各方中取得支持，使部门的整体基础设施保障工作顺利进行。

在实施教育和推广项目时，银行与金融部门要与财政部门密切合作。按照优先顺序，这一工作的主要对象应该首先是公共-私营部门的官员以及基础设施的所有者和运营者。其中，公共部门官员包括联邦、各州和地方的管理部门、立法部门和执法部门官员。对公共部门中的听众来说，除了推广国家安全和系统化风险的主题外，还要面向基础设施的所有者和运营者，向其传播有效的基础设施保障业务案例。

银行与金融部门将为各级基础设施的所有者和运营者制定合理的关键基础设施保障措施，以使这些人员能够采纳这些措施。为了评估教育和推广工作的有效性，必须对希望的结果进行定义并排定优先级别，还要建立绩效评估规范。绩效评估规范应该根据每个希望的结果和实际情况制定，并对此工作进行测试，以确保教育项目的有效性。研发项目是这项工作的一项有力补充，它是银行与金融部门中的一项的特殊领域，没有国家的相应资助。银行与金融部门将查看政府提议的研发工作，并向本部门提供反馈，便于本部门对研发优先级的确立。

## 4. 其他考虑

除了此前讨论的风险管理问题外，保险商以及法律、规章、执法机构、国际环境的角色也将对关键基础设施保障造成重要影响。

### A. 法律、规章和执法

银行与金融部门有两个关键任务：（1）确保银行与金融部门的职能不受恶意或偶然事件的影响，确保金融系统和国家经济有条不紊地运行；（2）继续保持公众对银行与金融部门防护、检测和响应能力的信心。立法和政策上的议程有助于实现上述目标。议程中应该包含以下五大问题：信息共享和公私合作领域的法律阻碍；客户对合理的安全措施与隐私措施的信心；部门范围内的危机和后果管理结构；立法和规章项目；法律 and 政策的修正和协调。

### 法律和规章

#### 问题 1：对信息共享和公私合作联盟的法律阻碍

##### （1）信息共享

法律和政策讨论的重点是信息交换和合作的重要性。作为一个法律问题，对信息共享的阻碍并不总是与少数问题有关。金融机构对共享工作的经验和能力，对特定的基础设施威胁、脆弱性和风险评估细节的知识和信息，都是政策的一部分，都是讨论的内容。<sup>①</sup>银行与金融部门、重要的利益方、政府部门要紧密联合起来，确定并消除信息共享工作面临的阻碍。

##### （2）合作

合作计划是大多数（即使不是全部）关键基础设施部门战略的内容。银行与金融部门为关键基础设施的跨国合作已经付出了几年的积极努力。本部门还希望与政府部门建立合作关系。在这方面，银行与金融部门的意向包括与银行法规的制定机构等监督金融服务活动的政府机构间进行直接的信息反馈和信息交换。法律和政策方面必须对这些工作给予支持，同时有可能要

---

<sup>①</sup> 自从关键基础设施保护总统委员会首先描述了信息共享和合作的绝对重要性后，银行与金融部门组成了合作联盟来改进基础设施保护状况。FS/ISAC 是第一个部门级的信息共享和分析中心。它在开发信息共享模式方面对其他部门提供了帮助。

求修改法律框架体系，以加强讨论和密切合作。

在基础设施保护的问题上，银行与金融部门必须继续改善合作机制。为了表明合作的力度，银行与金融部门首先提出了“合作竞争”的概念。合作竞争的含义是在保持传统市场竞争原则的基础上，还要确保对安全和风险管理事务的合作。这些提案必须得到法律和政策的支持。

国会、管理机构以及银行与金融部门的代表正在消除阻碍，鼓励信息共享与合作，通过重新审查某些法律和政策中的条例，进一步加强对基础设施的保护工作。这些法律解决方式形成了一个法律和政策的大环境，有利于金融服务各方之间自由和公开地进行信息交流，包括所有的金融机构、服务商和提供商以及联邦和各州的政府部门。

一些工作可能还需要国会的参与，包括对《信息自由法》（FOIA）中不泄漏条例的赦免，关键基础设施合作的反托拉斯条例赦免，以及对某些充分定义且重要的安全及基础设施保护工作义务的赦免。

有关大范围合作和信息交换的特殊工作需求在合作讨论中要引起注意，支持关键基础设施服务的金融机构等方面已经为国家活动提供了很多投资，用于开发基础设施保护方案。这些工作主要是以信息共享的形式完成的，如前面 FS/ISAC、BITS、ABA 等部门行动中讨论的内容。

这些活动有助于确保以安全可靠的方式提供金融服务。在关键基础设施领域，合作与信息交换是一个整体，法律和政策必须给予应有的支持。如上所述，在综合解决方案中将对会议、讨论和工作面临的阻碍进行细致检查。

#### **问题 2：通过合理的安全与隐私措施增强客户的信心**

客户信息的安全和隐私是银行与金融部门的一项核心目标。关键基础设施保护工作已经融入到国家安全、经济安全和国防安全。如果得不到客户的充分信任，银行与金融部门就不可能实现其关键基础设施的目标。因此，对客户信息和资产的保护也是国家安全目标之一。

最新的《Gramm-Leach-Bliley（G-L-B）法》的发布，以及用于确保 GLB 实施的法规，均使人们意识到了保护客户信息的重要性。OCC 等法规制定组织已明确表示，网络空间的安全工作是 GLB 工作的一个重要组成部分。GLB 也明确提出，这项工作在本质上是一个具有广泛责任的问题。在定义和实现合理的安全与隐私措施方面，银行与金融部门将继续扮演领导者的角色。其中的一个例子就是《BITS IT 服务提供商技术风险管理框架》，该框架的作用是解决金融服务组织间有关法规、业务和技术风险方面的问题。

银行与金融部门还将继续在改善合理和安全的措施培训方面起领导作用。通过各种各样积极的工作，银行与金融部门从整体上提高了人们对成功战略的认识。例如，美国银行家协会已为 GLB 安全保密工作开发了一套可广泛使用的工具。ABA 等其他协会则侧重于盗窃事件的识别，并为管理这些问题提供了解决方案。

#### **问题 3：部门范围内的危机管理与后果管理结构**

在某些有关管理结构的复杂领域，法律和政策环境必须协助并支持部门级对于管理结构讨论。非常明显的是，法律已经严重滞后于技术和商业发展。很多情况下，立法的缺陷也阻碍了业务发展，特别是在难以识别、检测和量化风险的领域。而在其他一些情况下，现有的法律也对合理的风险管理和安全事件措施造成了破坏或阻碍。安全合作工作中潜在的反托拉斯责任往往是行业成员在解决问题时最头疼的。

国会和政府应该对法律和政策进行协调，以使各基础设施部门能够开发管理项目、制定管理结构和过程。银行与金融部门尤其建议国会和政府：

- 研究本部门的准备、响应和恢复工作中的反托拉斯责任问题。这些工作比威胁和脆弱性信息的共享更具有广泛意义。司法部和联邦贸易委员会的管理性保护工作，如业务审查书和自愿性方针尚不能解决安全合作要求中的重大风险问题。
- 研究本部门的危机和后果管理活动中遇到的其他法律阻碍，包括在危机和危机之后的服务恢复工作中可暂不执行的管理和法规要求。
- 研究哪些立法项目可以促进本部门的准备、响应和恢复过程。此类例子包括：
  - 1950 年制定的《国防产品法》<sup>①</sup>及用来规定货物和服务分配的优先性的其他相关项目；
  - 国家安全/应急战备中的通信项目，如 GETS。<sup>②</sup>

#### 问题 4：立法和法规项目

保险项目和产品是管理国家安全威胁和风险过程中的重要元素。立法和法规项目应该在以下方面支持这一管理元素。

- 精算数据的产生：保险公司目前缺乏充分的精算数据来支持风险量化。因此，需要制定能产生精算数据的方法，以用于开发各种网络保险产品和项目。信息共享的阻碍，如问题 1 中所述，应该得到研究解决，以便于精算数据能在关键基础设施的所有者和运营者之间自由共享，必要时还包括政府与政府共享。只有完成了这项工作，保险行业才能有足够的数据提供完整的保险保证金。
- 风险模型：到目前为止，银行与金融行业仍缺乏指导风险量化的风险模型。政府资助的实体所使用的某些技术，如 Los Alamos 和 sandia 国家实验室的技术，可能有助于解决这一问题。
- 关键基础设施的互依赖性：最终，国会和布什政府应为基础设施互依赖性和事故的级联问题提供资金赞助。对于某单一事件可能因级联而引起的更多灾难性破坏，侵权和合同法尚无先例。因此，银行与金融部门将不断奋斗，努力研究综合性的风险评估方法，力争考虑到所有的风险。所有部门都可以从互依赖性及事故级联的研究中受益。研究结果对于改善风险管理战略也很有帮助。

#### 问题 5：调整和优化法律及政策

应在关键基础设施部门和政府间调整和优化法律及政策。其中以下几个领域需要密切关注和审查，以确保政府和行业间的合作。

##### (1) 国土安全

- 通过几项重大的法律、条令和管理工作，国会和管理部门迅速对“9·11”事件做出了响应。整个新的法律和法规体系对于银行与金融部门将会产生巨大而深远的影响。
- 国会号召本部门为打击恐怖主义做好准备。例如，PATRIOT 法的实施是大大建立在恐怖主义金融网络的识别基础之上的。某些情况下，立法会直接影响到其他部门，如航空部门的安全要求。国土安全所涉及的立法和政策领域将影响我们的风险评估和

---

① 对于私人拥有和运营的关键基础设施与《国防产品法》之间的关系，国会还在对其进行初步的研究。2001 年 6 月 27 日，参议院议员班尼特（R-UT）作为银行委员会的一个成员，请求布什政府向国会汇报《国防产品法》与关键基础设施保护之间的关系。

② 在某些危机事件中，“政府应急电信服务”将提供对电信服务的优先权。它们通常被第一时间响应人员，如警察和消防队所使用。由于银行与金融部门的关键基础设施保障目的，银行业也可以纳入这种服务的范围之内。



管理措施。

- 布什总体也号召我们制定管理国土安全、关键基础设施保护和信息安全政策的框架。<sup>①</sup>国土安全办公室和国土安全委员会的成立是二战以后美国行政管理部门最重要的一次重组工作。
- 最重要的是，美国第一次成立了网络空间安全办公室<sup>②</sup>，负责协调各部门和跨工业部门之间的主要问题。
- 在国会和行政管理机构完善立法框架的时候，银行与金融部门将与我们的高级领导人一起，将国土安全政策整合到我们的业务措施中来。

## （2）鉴别

- 政府和行业部门都在积极制定鉴别项目和政策。管理和预算办公室指导下的财政部已为《削减文书工作法》（GPEA）颁布了美国的鉴别政策。银行与金融部门将继续与政府官员合作制定本部门的鉴别政策。这些政策之间必须保持协调。
- 2001年8月，联邦金融机构的检查委员会（FEIEC）发布了对电子银行应用中使用鉴别技术的指南。FEIEC是一个跨机构的协调实体，由联邦储备委员会、联邦储备保险公司、现金控制办公室、廉政监督办公室和国家信用卡联盟管理局等部门的代表组成。该指南是FEIEC和各有关联邦金融机构管理机构发布的系列文件之一。在过去的几年里，这些金融机构都致力于鉴别技术的应用及鉴别服务的提供。
- Identrus 和 TrustID 是两家行业鉴别机构，负责鉴别政策和合同基础设施的制定。Identrus 是一家全球金融网络机构，而 TrustID 则由 ABA 和美国抵押银行家协会共同建立并资助。这两个机构将通过通用广为接受的数字证书的形式为 Internet 交易提供鉴别和安全保证。

## （3）信息安全

- 美国信息保障法律和政策必须与银行与金融部门在此领域的工作成果一致。银行与金融部门正致力于制定信息保障标准、指南和建议。随着政府面临的挑战的不断升级，确保不损害基于本行业特定情况而建立的风险模型及评估工作是非常重要的。银行与金融部门希望政府成立与银行与金融部门的工作群体，以细致协调这些领域的工作。

## （4）国际电子银行

- 为了改善安全和有效的电子银行业务，“银行监督电子银行集团巴塞尔委员会”制定了“电子银行的风险管理原则”。该报告中讨论了加剧电子银行风险的因素，包括安全和业务连续性计划。
- 除以上外，还有更多的有关法律和政策机构管理工作的列表，请参考附录 D（略）。

## 执法状态和方向

### （1）执法的新角色

传统上，从简单的信息交换到面对诈骗行为紧密的司法裁决工作，银行与金融部门与联邦、各州和地方的执法机构均有着密切的联系。这些工作的目的只是为了防御和响应地理上发生的

<sup>①</sup> 例如，可见总统令 13228《建立国土安全办公室和国土安全委员会》（2001年10月8日）（组成了国土安全办公室，作为总统内阁的一部份）。

<sup>②</sup> 总统令 13231《信息时代的关键基础设施保护》（2001年10月18日）（组成总统关键基础设施保护委员会）。

犯罪活动或进行法律裁决。随着信息时代的到来，科技越来越复杂，法律责任越来越模糊，社会活动的影响越来越不可预知，银行与金融部门要和地方及联邦的执法机构团结起来，共同面对这个既新鲜又陌生的环境。因为金融服务领域是网络化和全球化的，地方部门管理地方犯罪事务，联邦各机构也是彼此之间独立工作的，工作范围也仅限于已清晰定义了的的责任领域，所以这些问题的讨论将一直持续。本小节内容讲述了对新情况的历史观，说明了改善共生的合作关系的重要性。

与传统的国家安全问题中的威胁环境不同，信息时代中威胁的本质将通过不断变换、匿名和技术复杂性来刻画，而且通常在初期无法了解其严重性。事实上，本部门对高新技术的应用已经超越了使执法部门的帮助能力。然而，执法部门可以单独或联合其他民事实体，通过早期检测或干涉等活动，缓解和消除可能发生的级联威胁，如通过信息共享这种简单的方式引发的级联破坏效应。

当世界步入 21 世纪后，金融和电子犯罪事件也日益增多，发展成有组织的犯罪团伙，其中很多还是跨国团伙。由于低投入高利润的诱惑，更多的职业犯罪团伙也加入到了信息犯罪中来。这些年间信息犯罪的程度不断升级，究其原因是全球化和信息技术的革新，犯罪团伙因此有了机会以海外国家为根据地，用各种方式进行犯罪。他们的犯罪方式包括电子方法，例如，通过本地定购海外的电子器械，通过与国外阴谋家合作，利用不同国家间执法体系的差异——种种犯罪一言难尽。因此，传统的司法概念也应该更新，由于原有的司法含义已不能解决当前使用地理上无边界的信息技术所产生的国际犯罪问题。

很明显，执法机构必须调制其组织结构、调查方法和国际关系，以解决跨国犯罪问题。现有的事件报告体系、立法制度和国际合作关系已明显不能满足这些变革的需求。联邦的执法资源和培训工作日渐紧张，疲于维持知识和技术，以能够应付不断变换的信息犯罪战场。

为了成功地执行调查、拘捕和起诉金融犯罪或电子犯罪人员的战略，为了彻底捣毁金融犯罪团伙，必须采取以下步骤：

- 鼓励通过正式或临时的方式实现合作或资源的整合。
- 与金融行业合作，更加有效地使用有关技术来标识和矫正系统缺陷。
- 继续与海外犯罪组织团伙展开斗争。
- 在国家和国际的范畴进行培训。

近些年来，网络计算机和电子业务的迅猛发展为恶意活动创造了机会，包括网络入侵和分布式拒绝服务攻击。作为第一时间的相应机构，执法部门现已开始认识到其处于保护关键基础设施的“前线”。从这一角度说，金融犯罪事件的探员必须审查电子犯罪案件的初始动机，而不仅仅了解某 Internet 信用卡交易中安全破坏活动的本身。罪犯常利用先进的技术，以最常用的方式进行着诈骗活动，但也留下了犯罪证据。

根据计算机安全学会 2001 年的计算机犯罪和安全事件调查来看，在过去的 12 个月里，计算机入侵事件增长了 2 倍，而对服务器的攻击事件则增长了 3 倍有余。这使得银行与金融部门成为了攻击者的工作目标，迫切需要本部门向执法寻求对策和援助，无论是在信息安全事件的事前，事中，还是事后。

## （2）对新技巧设备和资源的需求

虽然不是所有计算机犯罪事件的调查都需要经过充分技术培训的探员，但是在大多数情况下，没有充足的计算机知识力量做后盾，调查工作是很难成功的。一般而言，若没有对被攻击

计算机系统的分析或没有对系统日志的审查，没有对 IP 地址或对电子邮件的跟踪，就很难确定可疑点。在这样的情况下，没有对计算机可疑事件的分析，也就不可能完成调查。

由于在犯罪调查中广泛使用了电子证据，通过高素质的计算机调查专家及时对受侵电子介质进行调查的需求在这几年激增。虽然这需要有合格且高质量的取证项目，但在很多情况下，执法部门还不具备此条件。因此，探员就不得不常借助外部资源来审查复杂案件。

在未来，对计算机犯罪案件调查的执法工作成功与否，主要取决于是否为其提供了必要的培训、工具、设备和支持，以识别、保存和分析电子证据。同时，执法部门还要改善资源的应用状况，防止入不敷出。

### （3）执法任务组的概念

执法任务组的概念是新式的合作中让人最看好的一项。这一概念为执法部门的新角色有了实际的设定，扩大了信息交换，并改善了与金融行业的关系。它包括多个执法机构的合作，并且加大了银行、通信和学术部门的参与力度。

这项非传统模型（或称“第二代”任务组）的一个范例是纽约电子犯罪事件任务组，下属美国特工处。它很好地将学术界和私营部门的力量与执法力量进行了整合，便于处理计算机犯罪案件。这一方法不但可以得出准确的调查结果，而且为信息共享和成功地防御战略提供了开放的环境，在学术界的帮助下，可以使得培训课程实现制度化。

“第二代”任务组的概念给基础设施的所有者和运营者提供了宝贵的思考和经验。因为它可以使人们了解犯罪趋势，便于调查和起诉，还便于人们了解防火墙等防御机制的性能，并找到此前没有被识别出的缺陷。通过为复杂案件提供技术咨询和协助，基础设施的代表还为任务组做出了自己的贡献。执法代表的多样性确保了司法工作中不会出现矛盾或阻碍。有了金融服务代表们的参与，任务组还完成了一项对自己非常重要的任务。此外，任务组还取得了广而告之的效果，在犯罪调查中起到了重要角色，并为解决信息威胁提供了工具、培训和资源，使这些问题能被控制在小范围，而不会升级为国家安全事件。

### （4）与计算机犯罪有关的联邦法律和机构行动

有关计算机攻击的联邦法律案件包含在《美国法典》第 18 编“计算机有关的诈骗等行为”中。法律授予了 FBI 和联邦特工处调查计算机犯罪事件的权力，事实上，它们经常处理对金融机构的计算机攻击。这两个机构还有各自数不胜数的责任，但对于联邦特工处，作为财政部的分支，一般侧重于有关破坏国家支付体系和金融团体的违法行为上。

在调查“白领”的案件中，FBI 有其不少的附属机构，同时还有集中处理信息诈骗和基础设施犯罪的机构。除此之外，司法部和 FBI 都采用了地区计算机取证实验室的概念来为执法部门服务。不幸的是，需要计算机取证服务的事件太多，而金融诈骗案件往往得不到最优先的照顾。目前，这些取证机构主要为收集电子证据而设计，以便用于后续的调查。

联邦特工处的电子犯罪特别代理项目（ECSAP）由接受过特殊培训的班底构成，负责向境内和国外的公司提供计算机法学支持及高科技调查协助，以确保金融犯罪案件调查的顺利进行。在与有关资深探员的密切咨询下，联邦特工处重点强调了对突发事件的响应和现场计算机取证的支持。ECSAP 还不能与 FBI/DOJ 的区域计算机取证实验室相比拟，但它却是个流动式的计算机取证和调查资源。

根据第 63 号总统令建成的国家基础设施保护中心（NIPC）是 FBI 内的机构，主要负责处理和交换关基础设施事件、预警和战略的信息，并协调有关关键基础设施和金融团体计算机攻

击事件的调查。

地方和各州的执法机构平时都会遇到计算机犯罪事件。然而，其各自的计算机取证和调查能力却不尽相同，该能力并不要求与部门大小或所占人口成比例。在某些领域，地方执法机构可能有特别先进的项目，如南加州的执法处（SLED），最近得到了充足的资金，用于建立州立计算机取证实验室和电子犯罪任务组，可作为联邦执法措施的有力补充。在此项工作中，州政府在建设州立计算机取证设施时起到了领导作用，并聘请了特工处和 FBI 的人员参与了其高科技任务组。

**部门行动：**银行与金融部门将采取措施，改善与执法部门的工作关系。同时，有关病毒信息、攻击地点和数据分析方法的常规交换将是扩大和优化工作关系的前沿力量。

## **B. 保险风险管理**

在银行与金融部门中，保险行业在保护国家基础设施不受信息威胁和识别盗窃的工作中起着举足轻重的作用。必须鼓励保险行业建立特色的网络风险保险管理政策，并配有相应的术语和根据风险管理质量而定的保险费用。保险行业必须完成以下三项任务：

- 通过高质量的独立技术公司提供损失防御或损失缓解服务。
- 在遭遇网络攻击或网络诈骗时，提供可靠的金融损失风险转移手段，对于可能承受的风险来说，保险费要适中。
- 提供事件后支持。

由保险提供商提供的损失防御或缓解服务包括在线或现场安全评估服务以及廉价或免费周边检测。这部分服务的费用应该计算到保险费用中去，或者作为降低风险的方法，最好是免费的。鼓励保险业与提供风险降低产品和服务的技术公司一起成立战略联盟，从中实现保险费的折扣，使投保人愿意投保，并能获得最佳的安全措施。

为了使效率最大化，必须鼓励保险业提供更为广阔的金融风险损失转移服务，使各公司在处理风险暴露问题中纳入合理的风险管理技术，从而减少法律诉讼、Internet 收入损失（由于拒绝服务攻击）和公司数据破坏所带来的金融影响。

没有公司理事会成员的广泛参与，国家关键基础设施的安全工作就不可能成功。公司主管应该以积极的态度管理信息风险，就像他们在对待“千年虫”问题上所采取的态度一样。主管投保的领导或官员要积极协助对董事会的培训工作，并在必要时修改保险术语和保险费，以符合董事会管理层在此方面的政策。

由于公众信心是国家经济活力的基石，因此保险行业应该通过提供事后的保险金来积极支持国家经济长久的稳定性。这类资金的例子包括危机通信服务，以帮助恢复客户、雇员、股东等投保人的信心。

**部门行动：**在转移重大网络事件的金融损失时，保险业常显得资金不够。银行与金融部门建议公共部门考虑与大规模网络灾难事件再投保有关的事务。

## **C. 关键基础设施保障工作中的国际问题**

### **银行与金融业的全球属性**

金融部门对美国来说非常关键，他要依赖于国内和国际不同层次的基础设施。金融机构面临的威胁是全球性的。这些机构要依赖于美国的国家基础设施、他国的基础设施和全球金融系

统组成的国际综合基础设施，同时，它们本身也是这些基础设施的一部分。

另外，很多大型的国内机构都要依靠国际市场和资本流，以实现其日常的资金流动。当美国全球性金融机构或美国市场中的非美国机构面临着全球威胁时，即使这种威胁不一定是直接威胁，也可能造成很大危害。

美国国民面临的风险不仅局限于美国内部的机构。很多国民及其资产的流动性日益增强，可同时在很多市场中运转，因此要依赖于很多国家及其业务基础设施。所以，需要考虑保护全球金融市场内美国国民的利益。

### **互依赖性**

金融机构与市场之间的紧密联系形成了其间的互依赖性。这种互依赖性所引发的系统化风险可能造成跨国交易网络的失效。例如，如果美国某金融机构被美国市场所依赖，但它却属于全球化运行模式，则来自其他国家基础设施的威胁将对美国金融机构造成破坏，根据其严重程度，还可能直接对美国造成破坏。

### **国际所有权**

很多大型金融机构已经成为跨国的大组织。这些机构根据当地的地方政策和法规制定自身的规章制度，以整体而不是个体进行规划。这些机构的总部（虽然有很多进行了拆分）设在某个国家，由股东控股，客户分布于全球各地。就多样性和本身的风险管理经验而言，这有着一定的优势。但是，它同样扩大了所面临风险的范围，同时部门的计划必须从根本上特地考虑跨国金融机构（如 SWIFT）以及不同地区的结算、清算和金融信息系统。

### **全球威胁**

金融机构必须解决威胁、脆弱性和风险造成的破坏，必须采取安全措施，以管理与下述情况有关的风险：

- 交换、支付、消息发送、清算和结算基础设施的系统化崩溃或国家利益的受损；
- 一般体现为跨国性质的逻辑安全威胁；
- 一般体现为国内（或限于国内）性质的物理安全威胁；
- 声誉被破坏导致客户对金融系统信心的下降；
- 信息污染/准确性；
- 拒绝服务；
- 通过直接处理程序（STP）来减少手工（人）的控制；
- 客户的隐私权和个人安全；
- 国家背景下的身份保障。

### **基础设施及其组件的来源**

很多金融机构都十分依赖来自其他国家或由其他国家管理的技术组件、产品、软件和服务。国内外的金融机构在开发标准和制定规章时，都会直接或间接地涉及很多国家的这些设备。

### **法律和法规**

在国际领域，立法和本部门内的规章的数量不断增多，这便要求增强金融机构的保障力度。某些情况下，立法和规章行动可以限制某些行为、信息流和服务的运行，以增强对保障的控制。而其他情况下，它们就起到了推动全球保护基线的作用，通过跨国的实体，如欧洲委员会、EU、

UN、G8 等，各国的立法工作可以得到协调。这些实体所涉及的立法和规章范围有隐私权、银行保密业务、数据保护、跨行的数据交流和服务可用性等，并尽可能以最小的资本需求来推动安全工作的发展，使安全工作涵盖运行风险和安全措施，保证安全风险的最小保险级别。

### 国家基础设施保护项目的互依赖性

大多数成熟的国家都正在开发国家基础设施保护方法。这使得美国的工作要有同步性，并在可能的地方主动干预这些方法的发展。这些国家基础设施保护项目应该联合建立一种方法，使全球金融系统可以以一种综合的方法运行和合作，而不是分离地展开保护。

部门行动：银行与金融部门将继续工作，保障通过国际司法机构对攻击事件进行调查和起诉，并以协调的方式进行。

### 地缘政治学考虑

社会、文化和政治的概念不可忽略。很多国家对安全、隐私和控制的文化取向是不同的，这会在国家工作中产生分歧，除非得到了协调。同样，很多在金融部门中还没有实施综合性隐私策略的国家可能会采取与美国公私合作方式不同的姿态。

除持续关注其他国家的工作外，为了推动美国的全球化，很多工作也已经展开。其表现形式有多种，通常是美国大型金融机构固有的全球属性的直接反映。其中尤其包括：

- FS/ISAC 和 WW/ISAC 两机构间的适宜的信息共享。WW/ISAC 是@lertNet 早期预警系统的一部分，由 FS/ISAC 负责运营。它在全世界提供了 500 多个信息点，共享内容包括 FS/ISAC 和 WW/ISAC 的成员在会议上的报告。
- 在国家间共享恐怖主义和信息犯罪的数据是必要的，如加拿大、澳大利亚和英国之间。在东、西半球和南、北半球范围内，很多其他类型的信息交换和执法合作已经开展，或已在建立阶段。
- 来自很多国家的立法和规章工作者中的代表。
- 参与巴塞尔委员会中针对电子银行风险管理的银行监督原则的制定工作。

### 国际化工作

银行与金融部门工作的国际化的焦点主要集中在不单独依赖于任何一个国家的全球金融系统的保护上，其理念在于，对一个国家的金融基础设施的保护，不论是其国内还是国际金融基础设施，都会对全球金融基础设施的持续健康发展带来影响。

#### (1) 国际化工作——部门计划

部门计划中的每项主要工作都会产生国际化影响。以下是其关键要素。

- 所有计划中的国际化工作必须包括以下内容：
  - 将一个国家的类似的关键基础设施保护工作映射到另一个国家中，以判断是否具备联盟、学习或共享的机会。
  - 研究全球金融机构的跨国性，推动美国金融机构与外国机构之间的结盟，或者通过美国境内的非美国金融机构进行结盟。
  - 为保障关键基础设施的保护工作，努力采纳、影响或创建国际标准、业务实践或其他框架。
- 为定义和开发合适的信息安全/关键基础设施风险迹象显示器，对其提供资金，以便配合未来的资金规划工作。

## （2）国际化工作——政府指南

下述内容定义了一种工作方法，如果能够在各国之间得到协调，那么大型金融机构的国家保障便可以得到和谐一致的支持。

- 强大的采购者。在越来越急迫的问题之中，市场技能的限制以及整体安全方案的不成熟首当其冲。就技能而言，面临的挑战不仅是安全专家在数量上的不足，更加急迫的挑战是其他学科中缺乏基本的安全知识。通过改善金融及其他机构的影响来刺激市场，政府及相关行业机构能提供更多的服务项目。
- 刺激管理环境。政府及其国家和金融管理机构可以通过建立合理的框架来改善安全工作，框架中要整合本部门中管理和立法等方面的安全意图。
- 业务环境的保护者。国家机构的概念已不复存在。仅仅聚焦于国家的“优胜者”将会导致分裂。政府要推动和帮助为所有的机构建立良好的业务环境，这将取得更好的国际效应。
- 伦理/教育和技能。一个希望具有安全性并积极努力的环境（无论当前如何定义安全），都会对国家产生长期的重大意义，这比中央政权的驱动要有效得多。一个期望具有安全性的环境一般要更擅长实现和维护安全性。
- 小型/中型机构的支持。与政府在刺激技能和技术/过程成熟性中的强大的采购者的角色相一致，可以采取类似的方法，通过刺激机构（尤其是中小型机构）的安全改善工作来推动市场。传统上，这些机构没有充足的资源像国际组织那样在同样范围内致力于安全工作。这些刺激应该是一种积极鼓励型的，而非强迫惩罚型的。
- 关键研发工作的长期赞助商。目前已有许多领域变得越来越关键，但很多领域中，工业界的关注不够，或者缺乏成熟性。政府部门可以引入一些需要重新讨论的课题，来刺激这一领域的研究工作。
- 非国家性商业合作。只有与不同地域的非国家性企业展开合作，才能有效地支持国际化方法。这应当是一种在全球级别上的政府与商业机构之间的合作。

## D. 互依赖性和相关风险

### 对其他基础设施组件的依赖性

在“千年虫”问题解决之前，应急计划中充满了世界末日的描述，虽然很多人怀疑这样的破坏性事件是否会真实发生。幸运的是，由于人们做了大量的减缓和准备工作，考虑到了非常多的意外情况，怀着超常的警觉性，并且通过一些措施幸运地发现并阻止了恐怖分子的计划，所以在“千年虫”期间并没有发生任何严重的灾难事件。然而遗憾的是，“千年虫”防御工作的成功使得一些美国公司沾沾自喜，直到 20 个月后这种情绪还在不断扩散。

2001 年 9 月 11 日，美国纽约的世贸中心和华盛顿地区的五角大楼所受到的攻击彻底改变了美国人对基础设施风险和互依赖性的理解。在纽约和华盛顿所受的袭击中，我们目击了其他基础设施部门的级联影响。而一周以后，这类影响则以网络空间中“Nimda”病毒的形式进一步恶化，在整个国家的范围内感染并破坏了计算机网络。之后，纽约和华盛顿地区又落入炭疽病毒的恐慌之中，这种恐慌随即影响到了整个美国甚至全球的人和公司。所有这些事件，就其本身来说当然是破坏性的，而一旦连续发生，所带来的影响便是一种极为恐怖的、几乎无以计量的损失。

通常认为，大规模恐怖袭击或自然灾害（如龙卷风、暴风雨和洪水）可能会产生地区性或全球性的恶劣影响。关键基础设施的很多组件可能会由于单一事件而受到破坏，也可能被来自同一攻击源的一系列事件所影响。

#### **“9·11”事件的直接和间接影响**

几架飞机同时被劫和世贸中心的撞击事件至今仍令人扼腕，这起恐怖行动的含义却远不止劫机和撞击事件本身那么简单。世贸双塔的坍塌景象仍历历在目，死伤的人不计其数。除此之外，一些通信设施同样受到了破坏，例如：

- 在双塔坍塌时，双塔顶端信号天线电波覆盖的电视台服务中断和蜂窝电话全部失灵；
- 由于双塔的倒塌，位于西经 144° 的纽约市区的多个建筑物（包括通信 HUB）被严重破坏；
- 纽约的指挥中心和美国特工处总部被破坏。

在通信设施受损的同时，曼哈顿地区的城市运输也严重受阻。除曼哈顿南部地区的当地居民和救援人员外，任何人都不得进入此地区。在接下来近一周的时间里，美国航空系统停运，股票市场关闭。

统计表明，16 英亩土地在这次袭击事件中被毁，曾经高度集中的金融部门不得不更换地点。虽然很多公司能够重新恢复设备，但是日常业务功能的损失仍然非常严重。正当公司努力在这种不利局面下运行时，一种名为“Nimda”的蠕虫病毒却火上浇油，阻塞了网络，使情况进一步恶化。之后的炭疽病毒迅速又以致命性的影响改变了人们对于传统邮件的看法，整个美国数以万计的邮件被截获检查。

银行与金融部门同样受到了与其股票经理人、清算银行等核心机构之间的通信和交付机制失效的影响。对于这一突如其来的灾难，即便很多公司制定了应急计划，但在这样的大灾难中，它们中很多无法奏效。所有这些事件及其余波说明了关键部门间普遍存在的紧密的互依赖性。

**部门行动：**在认识到上述事件以后，为银行与金融部门制定的关键基础设施保障国家战略必须统计关键部门（如通信、电力和交通部门）的损失总额，包括受牵连的组件和层面（如人员、建筑和家具）。

下面各小节将考查这些互依赖性所引发的风险。

#### **建筑物和物理风险**

物理设施面临的重大风险是导致其不能实现预期功能的某些事故。事故的原因有很多，当电力中断时，设施可能完好无损，但却不能访问，因为该站点正处在停运状态；在面临炸弹威胁时，由于设施的不安全也可能无法靠近。在火灾或洪灾发生时，建筑物可能会被部分或全部破坏。物理风险的另一类情况可能是由非授权访问引入的，这些非授权访问物理设施的人可能会对组织的员工和资产造成破坏。

在解决物理基础设施面临的威胁时，保护原则反映了网络计算环境的保护措施。建议使用多级保护制度作为避免或防御物理入侵的方法。虽然公司资源和需求的不同会导致工作内容和性质的不同，但是在选择保护机制时有很多方法可供选择。例如，对于设施来说，要求其外部不应该太显眼，即从外部难以了解其内部情况。要设置围墙，以防止可能装有炸弹装置的汽车进入建筑物。另外，还要使用摄像机等监视和检测设备，并配以警报装置。在建筑物中，要使用守卫、出入登记、刷卡旋转隔离门和生物认证等装置，以确定在建筑物内的人员的身份。类



似机场 X 射线和金属检测仪等扫描装置也可以用于人体、货物和信件的检测。

为了防止火灾、洪灾等引发的威胁，必须采取预防措施使风险最小化。解决这些威胁的方法包括气体泄漏报警、无烟政策、屋顶防火材料的使用等防护措施。还可以使用检测装置来提供早期的预警，并减少这些威胁的影响。

尽管使用了各式各样的防护机制，但是仍可能发生威胁公司物理基础设施的事件。因此，公司必须有能力降低这类事件的影响，例如，通过洒水灭火或水仓泵等装置来降低破坏程度。对于仅有部分物理资产受到威胁的情况，如部分电力或通信资源丧失，公司应配备冗余资源，其中包括燃料发电和备份通信装置，如蜂窝电话和电子邮件、双向寻呼机等。在解决大范围的日常业务工作被破坏的问题时，公司还要有应急计划。这些应急计划中必须包括后备地址以及在替代设备上开展公司重要业务的能力。

各公司必须逐步采取行动来保护其资产，并协调地方当局以及本部门内其他公司的防御战略；必须进行跨部门的合作，改善关键基础部门间的关系，如电力部门和通信部门。这对于在本部门内外进行信息共享同样有着重要的作用，特别是共享威胁和脆弱性的信息。

### 员工——人为因素风险

公司员工引发的风险和威胁要分为内部员工和外部员工两部分来讨论。内部员工一般指雇员，外部员工包括顾问、供货商、客户和大众。外部员工与公司的关系可能是正常的业务关系，也可能是完全独立的。

内部员工在破坏或影响某雇主的物理、信息、知识或货币资产时可能有多种不同的动机。某些情况下，员工或前任员工可能怀有不满情绪，或者出于金钱目的。这类员工往往有权访问公司的操作系统和计算机系统。有时，一个员工可能是某外部人员“收买行为”的受害者。犯罪人员会使用欺骗的手段说服内部人员泄漏保密信息，或执行非法行为，以帮助其破坏公司的系统和运行。

一种防止公司信息被内部行为不良人员泄漏的有效且重要的措施是对雇员、合同商和顾问使用监控程序。这是法律允许的能对个人和公司的信息进行联合共享的领域，对银行与金融部门、其他所有部门间以及政府机构都是非常有效的。

在某些地方，员工会面临高度的风险，特别是高级管理人员，有可能被绑架或暗杀，必须有防止此类威胁发生的技术和流程。建议其减少公开露面的机会，特别是不泄漏其行踪，配备保镖，在必要时通过保护性交通工具阻止任何企图在物理上威胁高级管理人员的行为。

### 数据保护——隐私权、保密性和完整性面临的风险

在处理数据问题时，必须确保其保密性、完整性和可用性。对一个金融机构的声誉和可信性来说，能否在面临各种威胁时保护客户的数据，尤其是保密信息，绝对是一条关键指标。一旦数据被破坏，就会丧失可用性，无论这是不满员工的蓄意行为还是某员工的大意疏忽。数据的完整性被破坏后，就很难判断这样的数据是否准确和可信。

数据盗窃是另一种风险。电子数据不同于以往任何形势的数据，因为它能被很快复制，而且不留痕迹。因此，由数据所有者授权用户访问和使用受限数据是非常重要的。访问安全要由一系列流程和技术来管理，包括强有力的鉴别方法和由防火墙及应用访问技术对服务的限制。

加密技术有助于确保数据被正确传送到不同的授权团体，确保数据不会在存储和传输中被篡改。同时，加密也使非授权破译信息变得非常困难，即便在它们获得访问权的情况下。

在上述的所有案例中，数据备份是非常重要的，因为它有助于数据被破坏后的重建工作。备份数据应该被安全存放在远处地点。

公司必须有工作日志，监控这些日志可以了解到可疑或异常行为。入侵检测系统和日志机制是用来跟踪计算机环境中的变化和威胁的两大重要方法。

从本部门的角度来说，对威胁以及数据库、操作系统和通信网络中的脆弱性进行预警是非常有益的。为了使对这些问题的响应更加有效，通过共享解决方案或防御战略来共同解决威胁和脆弱性问题可以收效显著。

### 系统

很多影响数据信息的类似风险也会影响计算机和网络系统，包括应用程序和系统软件设备。系统被破坏的原因可能是内外部员工的蓄意行为，也可能是大意疏忽。这种行为可以是授权的，也可以是非授权的。

以往的事例表明，各式各样的威胁将导致计算机系统被破坏，或是没有被破坏但不可使用。通常，只要计算机系统的部分数据被破坏或丢失，那么整个系统就不可用了，因为系统组件和模块之间是相互关联的。设备还可能遭受物理方式的破坏，从而导致失效。这种情况也将导致软件程序无法使用，从而使系统或部分系统失效。

公司通常会雇用第三方服务机构购买应用程序和系统、存储和传播数据。这就引入了另一种风险，因为公司所依赖的数据安全性、完整性和可用性掌握在他们无法直接控制的服务商手中的。

如今的一种趋势是客户和业务合作伙伴访问权限的扩大，如通过 Internet。这使得人们更容易访问内部公司系统，也使得公司的网络和系统面临的风险增大了。因此，公司要保护其周边环境不被非授权和未鉴别的访问者访问，并采取措施检测和响应入侵。一个减少系统破坏和误用的重要途径是细致管理对授权系统用户的鉴别访问。这样，一个高安全等级的系统就可以从智能卡或生物测定中获得足够的鉴别。系统管理的财产越多，关键程度越高，其安全性也就要求越高。

### 公用设备——基础设施的依赖

公司的运行要依赖于由很多公共设备构成的基础设施，如电力设施、通信设施、运输设施以及金融设施（如股票交换和清算机构）。由于很多组织所使用的公共设备的数量很少，因此任何设备的丢失都会产生严重影响。

对银行与金融部门来说，重要的是能确保其设施有足够的应付数量的巨大变换和要求的迅速变更的能力。公司不可完全依赖某特定的设备。例如，必须有代替电力和通信设备的设施。金融机构可以亲自或由第三方审查和评估这些设备，以确保其能够满足本部门的需求。

部门行动：为了保护设备不受破坏，确保部门的完整性，银行与金融部门需要共享有关威胁和脆弱性的信息，并在响应任何可能引发的问题是加强协调。

## E. 总结和摘要

法律、规章、执法和国际环境对银行与金融部门的关键基础设施保障工作有着重要的影响。为了保护金融系统的安全，银行与金融部门必须保持公众对其保护基础设施、检测和响应基础设施威胁和事件能力的信心。没有任何部门可以完全独立地工作，应使支持部门最大化地利用安全资源。

法律和政策可以帮助银行与金融部门实现其工作目标，银行与金融部门已经着手于此方面的工作。目前法律上的障碍使得信息共享和公共-私营合作联盟变得迫在眉睫。国会、管理局及银行与金融部门的代表正在审查一些特定的法律和政策，力图通过删除某些障碍并协助信息共享及合作联盟的开展来进一步实施基础设施保护工作。

另一个问题是如何保持客户对安全和隐私工作的信心。最新出台的 GLB 法和 GLB 执行法规已通过推行一系列规定来确保客户信息的安全，以期解决某些隐私问题。另一项法律问题涉及了部门的危机和后果管理结构。某些问题上，已有的法律损坏或阻碍了合理的风险管理和安全实践措施的实施。此外，安全合作中可能导致的反托拉斯责任问题一直是行业成员共同关心的重要问题，需要得到及时解决。

与规章有关的另一问题是信息风险的精算，它将影响保险公司能否提供合理有效的信息保险解决方案。在国家安全威胁和风险的管理中，保险项目和产品将承担起重要的角色。立法和规章项目必须协助精算数据的产生、风险建模以及关键基础设施互依赖性研究等工作，从而支持保险业在该领域的发展。最后，必须在关键基础设施部门和政府机构间协调和理顺各项法规制度。需要对某些领域密切注意和审视，确保政府和工业界偕同工作，包括鉴别、信息保障和国际电子银行业务。

历史上，银行与金融部门与联邦、各州和地方执法机构已经有很密切的关系。执法机构可以通过信息共享工作来使合作进一步密切，从而得以缓解并消除早期检测和干预中发现的潜在破坏性威胁。随着执法机构不断调整新的组织结构、探索新的调查方法和国际关系，以解决无边界技术犯罪问题，传统的司法概念需要被重新审视。执法机构对金融领域计算机犯罪问题的调查是否成功将取决于是否为调查机构提供了足够的探员、工具和设备，以及能否支持对电子证据的识别、保存和分析。

目前前景最看好的部署和合作工作是执法任务组的概念。任务组将赋予执法机构新的角色，扩大了信息的传播，加强了与金融部门间的合作。任务组的方法理念中，包括一个由众多执法机构联合组成的团体，还需要银行部门、通信部门和学术界代表的积极参与。“第二代”任务组的例子是纽约电子犯罪任务组，由美国特工处主持，它成功地将学术界、私营部门与执法部门联合起来，共同处理计算机犯罪事件。这种与执法机构的关系并不是单向的，银行与金融部门将研究是否需要进一步增强与执法部门的工作关系，其中包括对盗窃等消费问题中的信息的收集整理。另外，对于有关病毒、攻击地址和数据分析方法的常规交流将是在扩大和优化工作关系时最先需要解决的问题。

在银行与金融部门中，保险业也扮演了保护国家关键基础设施不受网络风险的重要角色。保险行业在促进风险管理工作上有其特殊的位置，因为它可以通过保险来提供保护工作中的资

金。应该鼓励保险商建立与投保人所要求的风险管理质量相匹配的风险保险政策。同时，保险商要履行下述三项基本义务：

- 通过高质量的独立技术公司提供损失的预防和缓解服务。
- 在发生攻击或诈骗事件时，提供合理的金融损失风险转移策略。
- 提供事后工作的支持。

在处理关键基础设施面临的威胁时，银行与金融部门必须考虑到各种各样的全球影响和因素。很多美国公民及其金融资产日趋流动，并同时在很多市场中运行，依赖于很多国家和商业基础设施。美国国内很多关键的金融机构也要依赖于各级的国家和国际基础设施。这些设施的集合就形成了全球的金融系统。金融机构和市场间的紧密联系造就了二者的相关性，并增加了系统化风险，可能导致国家网络主要组件的故障。到目前为止，除了继续与其他国家保持联盟外，本部门已经进行了很多工作来增强美国安全工作的全球化。

社会、文化和政治见解是不可忽视的。在安全、隐私和控制等问题上，很多国家有自己不同的观点，如果这些观点不能相容，那么将导致各国工作的不一致性。同样，很多国家已经对银行与金融部门展开了全面的私有化工作，它们可能会采取与美国的公共-私营合作联盟方法不尽相同的方式来部署安全工作。银行与金融部门将继续保障对攻击事件进行调查和起诉的国际工作能够以一种协调的方式开展。本部门工作的国际化的重点是保护全球金融系统，这一全球金融系统超越了任何单一的国家。银行与金融部门认为，对一个国家的国内外金融利益保护，从本质上讲与全球金融系统的稳健是分不开的。通过在全球金融的大环境下工作，银行与金融部门将更好地解决美国关键基础设施面临的威胁、存在的疑惑和脆弱性。

---

# 十一、信息与通信部门的关键基础设施和 网络空间安全国家战略（摘要）

美国信息与通信部门

2002 年 5 月

---



扫二维码阅读全文

## 执行摘要

信息与通信部门的人员和物理设施均在“9·11”事件中遭受了严重损失。很多专业管理人员和技术人员牺牲了生命。他们分别来自 Akamai、Accenture、BEA Systems、Cisco Systems、Compaq、GENUiTY、Metrocall、SAIC、Wipro、Oracle、SUN 和 Verizon 公司。财产损失则来自遭受破坏或者彻底丢失等厄运的计算机、软件和数据。据估计，在“9·11”事件中，仅金融行业所损失的 IT 资源就达到 32 亿美元。来自 Morgan Stanley 的统计结果则表明，该事件对 IT 硬件、服务恢复、企业长期的 IT 投入和世贸中心的年度 IT 支出所造成的损失则高达 250 亿美元。

信息与通信部门是一个由众多的人员、技术、产品和服务共同组成的庞大团体。但是，该部门在灾难发生期间的表现非常出色，在遭受打击后也将变得更加强大。

“9·11”事件充分表明，信息与通信部门是国家关键基础设施的一个重要组成部分。因此，它可能会成为美国的敌人在今后对美国实施攻击的主要目标之一。为此，信息与通信部门必须积极行动起来，保护关键的信息与通信资产。这些资产既包括该部门自身所采用的信息与通信产品和服务，也包括它为其其他工业部门提供的产品和服务。

PDD63 命令各部门制定各自的基础设施保护计划，并且下令设立私营工业部门的协调机构。信息与通信部门中承担此项职责的机构有以下四个：移动通信与 Internet 协会（CTIA）、美国信息技术协会（ITAA）、电信工业协会（TIA）和美国电信协会（USTA）。

本文第 1 章概要性地说明了关键基础设施保障问题，并且确定了为保障运营连续性而需要采取的行动。它指出本部战略的目的是：

- （1）提供对于信息与通信部门中的技术和业务环境的理解。
- （2）从广义上定义与该环境相关的威胁与脆弱性。
- （3）澄清信息与通信部门当前和未来行动与关键基础设施保护的联系。
- （4）揭示今后为保护信息与通信基础设施所需付出的努力。

本文也确定了信息与通信部门的一系列“第一原则”。这些原则必须指导以实施关键信息基础设施保护为目的的后续行动。

第 2 章结合信息与通信部门的实际情况考虑关键基础设施保障问题。此时，必须从现实的观点出发，以便形成一个该部门内部清晰一致的保障方法。信息与通信部门必须对自身的运营实施保护。同时，它也必须意识到，它为其其他部门提供的产品和服务已经成为这些部门保护其基础设施资产所依赖的基础。因此，它必须在对第三方的攻击做出预测和响应的同时寻求商业解决方案。此外，它也必须考虑客户要求的演变、产品更新、新技术和新的商务模型。本文探讨了威胁、脆弱性、互依赖性和有关风险的管理问题。

第 3 章说明如何确定有关各方的角色和建立合作关系。信息与通信部门由规则的和不规则的两类元素组成。本文的目的之一便是确定关键基础设施保障任务中应该由工业界决定并得到政府支持的部分，以及必须得到政府更积极的参与的部分。因此，不仅需要考虑到法律问题对关键基础设施保障可能造成的影响，而且必须考虑公共-私营联盟的关系及其作用。

第 4 章考虑了未来的情况。信息与通信市场具有其不断的变动性。商业运行所依赖的信息与通信产品和服务的更新换代也非常迅速。对这个市场上不断推出的新产品与新服务，人们往往难以做出预测，或者仅能依靠丰富的想象力进行缺乏准确性的猜测。信息与通信部门必须在

目前以及未来的日子里时刻准备着采取必要的行动来保护关键基础设施的各组成部分。

## 1. 背景与范围

在最近 50 年里，信息与通信部门已经成长为国家关键基础设施保护的组成部分之一，并且成为全球经济增长的重要驱动力。因此，它也成为未来可能遭受攻击的主要目标。该部门承担着保护国家关键信息与通信资产的任务。这些资产既包括该部门自身所采用的信息与通信产品和服务，也包括它与其他工业部门提供的产品和服务。本文概要地描述了关键基础设施保障问题，并解释了工业界和政府为保障运营连续性所需采取的一系列步骤：

- 介绍信息与通信部门代表性企业中的四个部门协调机构。
- 描述信息与通信技术工业的主要市场与经济发展趋势。
- 定义本部战略的目的和目标。
- 确定信息与通信部门以保护关键信息基础设施为目的而设立的一系列“第一原则”。

### 背景

1997 年 10 月发布的《关键基础设施保护总统委员会报告》再次确认了信息与通信部门对国家经济至关重要的事实，并强调所有的关键基础设施（如分别由政府或私人经营的能源、银行与金融、交通运输、水力系统、应急服务）对 IT 与通信系统的依赖性正逐渐加大。该报告建议在公共-私营联盟和信息共享的基础上确定一个综合性的项目，用于削减脆弱性，保护包括信息与通信基础设施在内的关键基础设施。

### 部门协调机构

PDD63 任命美国商务部为国家关键基础保护的领导机构，同时也任命国家电信与信息管理局（NTIA）为信息与通信部门的部门联络机构。作为美国政府中负责信息与通信部门的物理与网络空间保护事务的领导机构，NTIA 已经通过基础设施安全合作组织（PCIS）与信息通信部门进行了密切合作。1999 年 2 月 25 日，商务部副部长 Robert Mallet 宣布成立了私营部门协会联盟（包括美国信息技术协会、电信工业协会和美国电信协会）。这些新成立的机构将作为信息与通信部门的部门协调机构。随后加入的移动通信与 Internet 协会也成为协调机构之一。

上述四个协调机构代表了信息与通信部门中各方的利益，由此确保了联盟在该部门具有广泛的代表性。

### 信息与通信业务

美国是信息与通信技术（ICT）产品和服务的世界领袖，占据了几乎 35% 的全球开支。自从 1993 以后，美国花费在 ICT 上的开支增加了大约 70%，到 2001 年超过 8 100 亿美元<sup>①</sup>。

信息技术已经成为一个令人难以置信的强大工作源泉和工作增长点。大约有 1 000 万人从事 IT 工作，以此谋生。这其中，有 85% 的人的雇主是小型公司。这一数字包括了 IT 业内部和

---

<sup>①</sup> 资料来源：Digital Planet 2002, World Information and Technology Services Alliance and IDC, February, 2002。

外部的公司。在美国差不多有 14 000 个 IT 公司，每个公司平均雇用了 50 个或更多职员<sup>①</sup>。

IT业以其重要的方式对美国经济的成长做出了贡献。依据商务部的数据，IT业总计整整占了全部实际经济增长的三分之一，并且占据了1995—1999年期间全部生产力增长的一半。1995—1999年期间，IT以平均每年度使计算机价格下降26%遏止了经济膨胀。

以客户的观点来说，金融服务业是IT产品和服务的最大消费者，在1999年内花费了超过700亿美元。这一行业紧随通信服务（617亿美元）、制造业（569亿美元）、批发（501亿美元）、贸易服务（412亿美元）、零售业（187亿美元）、房地产业（171亿美元）、运输（168亿美元）。1994—1995年间，运输业和贸易服务经历了IT开销达年平均24%的最高比例，紧跟其后的是房地产（17%）、金融服务业（14%）、通信服务业和批发业，均在12%<sup>②</sup>。

由于计算机硬件、软件和通信的实时应用，创立了在家工作的机会。毫无疑问，集中将是一种未来趋势。联邦快递公司和Hertz等公司正充当着这次运动的急先锋。

### 电信工业

电信工业的发展速度要比整体的经济增长速度快。为了推动电信业的成长，必然需要在技术方面投资，以提高客户的认可度并使客户的业务运营变得简化。过去，服务提供商带宽和容量中投入了很多，而今它们正在为增值服务中的软件和应用进行投资。在运输市场和现在这样一个高利润的竞争中，服务提供商正在利用这些应用来提高自己的竞争力，努力实现产品和服务的客户化，以此加强客户的信任并创造新的盈利点<sup>③</sup>。

美国电信市场（包括设备和服务）在 2000 年实现了 12.5% 的速率成长，产生了 6 092 亿美元的收入。其中，在电信设备上的花费继续以两位百分数增长，超过了 1999 年的 13%，达到 1 598 亿美元。2000 年在运输服务上的花费达到 2 876 亿美元，超过了 1999 年的 8.9%。

企业花费在设备和软件上的开支达到了 921 亿美元，网络服务提供商的开支达 532 亿美元。对带宽的继续要求促进了高速 Internet 的发展，IP 语音（VoIP）、网络集中以及高级标准的应用将继续驱动设备市场，这弥补了无线基础设施和语音通信设备花费方面的下降值。

有些因素将会影响电信业的性质及电信基础设施，包括网络集中、下一代网络（NGN）、对 IT 和电信的业务依赖性以及 IT 和电信业参与者的合并。下面简单介绍其中的某些因素。

#### （1）网络集中

近几年，电信业的成长主要集中于纯粹的数字化手段方法，如 IP 和 ATM 协议的实施。电路交换网络仍然承载了重要的通信流量，但是趋势正向着数字化方向延伸，过去的电路交换将被纳入组合或“集中”的结构中。这个集中网络将会保持传统电路交换网络的本质要素，并试图合并那些可适用在新的结构中的要素（如宽带光纤设备），还将废弃那些没有用的内容（如电路交换系统）。基础性的重要服务，如操作员援助、备用计费装置、长途免费呼叫和应急服务（如 911 服务）将会被保留。因此，这个未来的集中式网络将是一个真正异构的，并能达到客户期望的效果，以智能化的透明方式实现数字传输，而且还可以根据用户的需求决定是否提供网络情报资源。

上述文字描述了未来的发展趋势，一些旧的网络仍可能会在其中保留下来，也可能被抛

---

① 资料来源：When Can You Start?, The Information Technology Association of America, April, 2001。

② 资料来源：The Precursor Group, Independent Research, April 11, 2001。

③ 资料来源：“2001 Multimedia Telecommunications Market Review and Forecast”, TIA, January, 2001。



弃。情况总是动态变化的，而且将来仍会动态发展。

### （2）下一代网络

网络的发展，更准确地说是一系列互联网络和设备的发展，将对技术和业务的革新提供强大的推动力。多年以来，竞争模型也已经有了发展，允许越来越多的公司与传统的电信服务提供商互联。这种互联呈现了很大的多样性，需要确保必要程度的网络安全。另外，当联邦通信委员会和各州的管制委员会在审查已有的规章并考虑新要求时，应关注国家级的安全政策。

为此，1996 年《电信法》要求不同运营商实现互联。这样，在带来巨大利润的同时，大量的可用通信路径还有网络具备了韧性和持久性，使之能够对抗各种原因引起的攻击。我们面临的一大挑战在于如何评估和理解多个运营商互联后对网络可靠性和服务透明度带来的影响。

### （3）公司间的合并

在当前的环境和经济状况下，服务提供商之间的高度竞争可能会带来不同的结果——促进新公司的诞生，或者使某些公司最终消亡，也可能使多个公司合并成一个公司。在电信业迈向未来时，始终会伴随这些悲欢离合。

## 目标、目的与适用的读者

本篇计划的目标是提供对信息与通信部门的技术和业务环境的了解，以全局的观点定义威胁和与脆弱性，并清晰地说明 I&C 部门为保护关键基础设施而已采取或正在采取的行动。此外，本篇计划还指出了为保护 I&C 基础设施而需在将来进一步投入的努力。

本篇计划的目的是提供基础设施的全面理解，了解基础设施保护的方方面面，并建立一套程序来确保能标识、实现、维护或在必要时更新保护措施。

## 行动倡议

信息安全是国土和经济的安全的关键。国土安全中，网络空间防御的动力来自于工业界与政府之间正努力建设的合作联盟。在考虑的新旧技术以及竞争和法规环境后，I&C 部门采用了很多方法来解决关键基础设施保障的风险。I&C 部门表示，至少要尊重下列各项事实和原则：

- 工业界拥有并运营着大部分的 I&C 基础设施，因此，保护和安全问题是 I&C 部门的天职。
- 政府和工业界在 Internet 和电子商务的健康成长上，具有共同的利益，必须找到共同的基点来协调关键信息基础设施保护事项。
- 联邦、州和地方一级的政府实体在向工业界下达新的要求之前，需要妥善协调其国家安全活动，避免重复的、不必要或不一致的要求。
- 必须使各方能信任 I&C 基础设施是安全的。
- “网络空间伦理学”必须成为 Internet 词典中可以理解的词汇之一。必须在家庭、学校和工作地点宣传在线伦理的重要性。

因为 I&C 基础设施是一种全球性的通信媒介，国界在这里是透明的，所以基础设施保护是一个需要以全球方式加以解决的问题。

网际犯罪威胁的性质是动态的。关键基础设施保障需要工业界和执法部门在世界范围内的不断承诺、关注及合作。

I&C 工业界对网络安全行动的呼唤不仅仅基于其自身的经济需要，还必须在国内外的活动中遵循我们国家的关键基础设施政策目标。

## 2. 威胁、脆弱性与风险管理

在所有的关键基础工业中，I&C 部门是唯一在其本身运营及对外提供产品与服务这两方面都离不开关键基础设施保障的行业。这其中的挑战令人生畏。I&C 部门的公司必须开发关键基础设施保障的解决方案，然而，这些解决方案同时又会变成第三方的靶子。其间，客户的信息安全需求多种多样，产品的变化速度也很快，新的计算模式（如无线数据）又为流行的业务实践及信息体系结构增加了变数。本章将研究威胁、脆弱性和与其关联的风险管理问题。尤其会讨论下列主题：

- 多维的威胁属性；
- 威胁是如何放大的；
- 脆弱性评估；
- I&C 部门的活动；
- 部门间的互依赖性；
- 信息与通信部门的风险减缓活动。

### 威胁与脆弱性

“9·11”这个令人毛骨悚然的事件考验了 I&C 部门对大规模破坏的抵抗性。因为联网的人数和机构越来越多，对信息与通信系统的威胁正在稳定上升，而我们对这一情况还没有完全摸透。政府和工业界一样，正在变得更加依赖 Internet 上的关键服务。这种依赖不但增加了这些机构对电子攻击的脆弱性，而且加剧了这些攻击可能造成的损害。Internet 的迅速成长大大增加了潜在攻击目标的数量。

在这场灾难中，信息与通信部门——一个由人员、技术、产品和服务组成的复杂的网络做出了辉煌的响应，该部门遭受了打击而且坚强地挺了过来。

遭受厄运的美国人以及美国联合航空公司航班的第一个乘客电话，都说明信息与通信技术在进行应急援助方面扮演了的关键角色，I&C 部门使当局迅速了解了事件的规模，并紧急应对了这次国家级的突发事件。世贸中心遭受攻击后的余波中，语音、数据和视频通信成为危机时刻了解灾难的范围、指导救援行动并寻找失踪人员的重要手段。当然，我们也遭到了不幸事件：一些必需的通信基础设施在事件中化为乌有：

- 位于曼哈顿西街 140 号的 Verizon's 交换办公室支持的 350 万条线路遭受了严重的损害。Verizon Wireless 公司损失了 10 个蜂窝发射站点。
- AT&T 公司损失了世贸中心的光纤设备，位于附近一栋建筑物中的交换设备也被损坏。令人吃惊的是，AT&T 公司位于世贸中心地下室的交换机还能继续工作。
- Internet 服务提供商 Earthlink 损失了位于市中心区域的 14 个拨入号中的 2 个。
- 纽约市 Sprint PCS 公司的无线网络损失了 4 个基站。
- Cingular 损失了 6 个曼哈顿基站。
- WorldCom 公司损失了位于世贸中心地下室的 200 个高速线路上的服务。

一位 AT&T 公司发言人称华尔街附近 1 平方英里地带为“世界上汇聚了最多电信公司和设

备的 1 平方英里<sup>①</sup>。”

9 月 11 日的事件证明，通信工业有时候会遇到巨大的伤害。在那天早晨 9~10 点之间，《纽约时报》、CNN 和国家广播公司等新闻网站全部瘫痪<sup>②</sup>。Internet 上的通信量骤减，来自最流行的电子商务网站的平均响应时间从平时的 2.5s 延长到了 7s<sup>③</sup>。美国在线公司的即时报文积压了 12 亿份，相当于正常情况下的 100 倍<sup>④</sup>。据 AT&T 延长报告，在正午之前长途通信量翻了一番。Verizon 公司也说曼哈顿的呼叫量大概是正常数量（1 天 1.15 亿）的 2 倍<sup>⑤</sup>。Cingular 的呼叫则增加了 400%<sup>⑥</sup>。

但 I&C 部门保持住了底线，虽然发生了这样大规模的破坏性事件，但在曼哈顿、弗吉尼亚、阿灵顿、五角大楼攻击的现场，电信部门仍能运转。Internet 给附近数以百万计的使用者提供了一条可能的路径，使他们能绕过受阻或破坏的纽约线路，给狂乱的民众提供了寻找家人的途径，如提供电子邮件、即时消息、IP 电话呼叫等服务。

在这其间，通信服务提供商不得不手忙脚乱地为其光纤网络重新划定路由并重新布线。一些公司为灾难场所的工作人员提供了无线电话。攻击发生后的一个星期，Verizon 公司宣布，它已经恢复了 350 万条数据线路中的 140 万个，并且纽约证券交易所 15 000 条线路中的 14 000 条也恢复了电话和数据服务<sup>⑦</sup>。在恢复运营的第一天，它处理了 23.3 亿笔交易，且没有发生事故。事实上，纽约的很多客户发现，他们的通信问题不是来自被摧毁的电信硬件，而是来自电力供应故障。

对 I&C 部门的威胁分为不同类型。多数事件是故意打断或干扰计算机使用者。例如，很多“脚本小孩”<sup>⑧</sup>使用公开的黑客工具便可以造成骚扰行为，当这还不是真正的破坏性攻击。可是，有限的知识和有力的工具一旦组合，其中的风险就不可同日而语了。例如，同时向一个电子信箱发送数以千计的电子邮件便可以引起分布式拒绝服务（DDoS）攻击，导致服务器瘫痪和网站宕机；病毒、特洛伊木马和其他类型的恶意代码可以将危险的计算机软件安装到计算机中，故意非法使用计算机上的文件和数据。其他的在线入侵还包括故意诬蔑和损毁网站的形象、张贴政治信息或辱骂某个特定的团体或机构。这些损人不利己的攻击造成的损害或许能达到数百万或数十亿美元。

是什么激发了这些攻击者的行为？黑客可能视攻击为技术挑战，或者希望借此引起他人的崇拜，也可能仅仅是在兴奋中纵容一下而已。除此以外，有些攻击可能代表了某些怀有不可告人的企图的国家或组织。

有些攻击者希望通过入侵来偷窃有价值或敏感的信息，包括信用卡号、社会安全码，甚至是完整的身份信息。有时目标还包括贸易秘密和专属信息、医疗记录或金融交易信息。

① 资料来源：IDG News Service, “Carriers Report Steady Recovery in Manhattan”, Scarlet Pruitt, September 21, 2001。

② 资料来源：Network World, “Internet, Telecom Networks put to Test in Wake of Terrorist Strikes on U.S. September 17, 2001。

③ 资料来源：Internet Week, “Site Operators Regroup”, L Scott Tillett and Tim Wilson, September 20, 2001。

④ 资料来源：Interactive Week, “Safety Net”, Randy Barrett et al, September 17, 2001。

⑤ 资料来源：zDow Jones, “Verizon Says It’s Ready for Trading”, September 18, 2001。

⑥ 资料来源：Computerworld, “Nation’s Networks See Sharp Volume Spikes After Attacks”, Bob Brewin, September 17 2000。

⑦ 资料来源：Dow Jones, “Verizon Says It’s Ready for Trading”, September 18, 2001。

⑧ 指不慎熟练的攻击者。——译者注

对于一些网络罪犯而言，Internet 是向孩子散播色情文学的途径和用于助长儿童和成人的其他罪行的工具，包括欺骗、诈取钱财、赌博、贩毒、洗钱、虐待儿童、绑架等。

网络恐怖分子可能使用 Internet 来作为攻击物理的基础设施（如发电站或飞机场）。正如我们已经在中东和其他地区看到的那样，网络恐怖分子鼓励政治冲突和国家冲突，并能迅速地将 Internet 设置成一个团体对抗另一个团体的工具，使正常的社会陷于混乱。

不幸的是，另一类网络罪犯通常是内部人员违规进入系统内并窃听、篡改甚至抢劫公司的 IT 资产。原因可能是雇员因为受到工作单位的批评而寻求报复，或是为了获得同事的尊敬，也可能是在未授权的情况下“测试”公司的安全状况。

无论属于哪种类型，都可说明威胁是真实存在的。Asta 网络公司 2001 年的一项研究和加州圣地亚哥大学的试验都表明，通过观察一个极小的地址片段，在一星期内发现有攻击者针对 5 000 个目标实施了 13 000 次 DDoS 攻击。在测试周期中，多数目标只被攻击了几次，有些目标则遭受了 60 次以上攻击。对于很多小公司，在遭受这种网络攻击后的一周之久业务状况才能逐渐好转。

计算机安全学会/FBI 的一份用于研究计算机破坏情况的报告《计算机和安全调查》也证明了这个状况。2002 年，在调查了美国国内共计 503 个安全从业者、政府机关、财政机构、医学机构和大学之后，该报告指出：“来自计算机犯罪的威胁和其他信息安全破坏持续不衰，且引起的金融损失正在上升。”<sup>①</sup> 90% 的回答者（主要是公司和政府部门）称“在最近的 12 个月内，发现了计算机安全破坏”；80% 的回答者承认“由于计算机被破坏而遭受了金融损失”。<sup>②</sup>

2001 年 12 月 11 日，ITAA 公司和 Tumbleweed 公司发布了题为“保持信念：政府、信息安全和国土防御”的公众意见调查结果。该调查显示，超过 70% 的美国人关心 Internet 和计算机安全；另外的 74% 的人表示他们担心 Internet 上的个人信息被怀有恶意目的的人窃用；同等数量的人说，他们担心网络攻击可以破坏类似于电话网络或发电厂的关键基础设施资产。

- 35% 的人说他们“非常关心”Internet 和计算机安全，36% 的人说他们“有些关心”。
- 三分之一的回答者说他们对 Internet 个人信息被偷窃或误用“非常焦虑”；41% 说他们“有些焦虑”；78% 的应答者说他们“非常”或“有些”关心由政府掌握的个人信息可能会被滥用。
- 74% 的应答者表达了对恐怖分子使用 Internet 攻击关键基础设施的可能性感到烦恼。其中 37% 说他们“非常”关心，但另外的 37% 说他们“有些”关心。
- 尽管有上述的担心，但应答者没有在“9·11”攻击或恐怖战争后对其在线行为进行大的改变。只有 5% 说他们使用 Internet 时“在非常多的情况下”是为了更新资料和信息，34% 说他们对 Internet 的使用停止了一段时间。7% 的被调查者表示，自从 9 月 11 日悲剧发生以后，他们“很少”使用 Internet。
- 同样地，即使发生了炭疽事件，电子邮件也没有代替传统的纸邮件。55% 的人说他们没有改变电子邮件的使用情况；35% 的人说他们在使用传统邮件的同时也使用电子邮件；只有 3% 的人说他们已经决定使用电子邮件并避免使用纸邮件。

---

① 资料来源：Computer Security Institute Press Release, April 7, 2002。

② 资料来源：Computer Security Institute Press Release, April 7, 2002。

- 调查为联邦官员同时带来了好消息和坏消息。虽然只有 17% 的人表示对美国政府对抗网络攻击的能力“完全有信心”，54% 说他们有“一些”信心，但只有 17% 说他们“基本没有信心”。这种对“大哥”<sup>①</sup>的担心似乎非常轻微。很少有人调查中担心在“9·11”之后的环境中，他们的电子邮件将会受到政府的侦察。只有 10% 的人说他们“非常”担心联邦主管当局监听或阅读他们的电子邮件；同时 14% 的人说他们是“有点儿”担心。

除了来自外部的对关键信息基础设施的威胁外，风险还存在于网络自身，其中既包括与逻辑体系结构相关的风险（如广泛配置的软件和协议），也包括物理体系结构和安全措施（如建筑物周边安全）的脆弱性与不足。间接的风险则产生于缺乏对网络安全的关注，因此需要在大学和国家实验室进行威胁建模和仿真方面的投资。

物理资产的集中带来了单点失败的可能性。这与人口和工业活动集中的历史一致，其损失额度会非常大。

此外，没有实现提供商的多样性以及存储方式、交换设备、电信网络和电力支持等方面的冗余和备份，这也是风险的来源。

除了物理安全问题外，很多广泛使用的关键协议，包括域名系统的伯克利实现（DNS/BIND）以及路由协议、边界网关协议（BGP）中存在广为人知的缺陷，这已经促使人们投入大量精力去进行研究（目前这些研究还未完成），旨在为这些关键代码开发出新的安全版本。很多志愿性的技术标准团体（如 IETF 正在研究安全的 BGP）和私营公司都在为之投入，目前进行顺利。

除此之外，“理论上的”风险还来自于在安全研究和开发中的投资的不断失败。国家实验室和主要的大学在计算机仿真和建模能力方面的工作，可以帮助国家了解和响应这些研发中包含的系统化风险。

还有其他多种因素加剧了威胁：

- 不断引进新技术增加了无法预见的复杂性。
- Internet 的无边界性和法律的局限性为预防和检测网络犯罪带来了困难，为攻击者创造了避风港。
- 不明朗的动机和匿名活动使得难以追查在线犯罪。
- 主管人员不关心和缺乏安全意识，限制了对信息的资源投入。
- 掌握了必备的信息安全技术的职工的数量不足。

### 脆弱性评估

信息和电信系统是优先权很高的关注对象，不但因为它是我们国家、国际和经济安全广泛依赖的基础设施，而且还因为它是各种信息的传输、存储和处理的基础。I&C 部门代表着一个高度动态和竞争的市场，提供了众多的技术解决方案。客户将基于性能、适配性、可扩展性、可靠性和价格等方面来采用这些解决方案。同样地，基于市场需求，解决方案可能会将具备较好的信息安全性能作为自己的特色，而有的解决方案却不一定把安全性放在首位。例如，金融或石化工业的关键基础设施保障需求便与时装或食品服务行业的需求不尽相同。业务决策者必须进行折中考虑，因为安全并不可能总意味着成功。I&C 部门中的风险管理正在变得非常复杂。

---

① “Big brother”（大哥）是美国人对政府的戏称。——译者注

在 I&C 部门，总统国家安全电信咨询委员会（NSTAC）最近几年一直在评估通信基础设施的脆弱性方面非常活跃，尤其是公共交换电话网（PSTN）和下一代网络（NGN）。评估时包括了对物理、运行和技术方面的脆弱性的考查。USTA 已经在 1982 年后成为了 NSTAC 的一个成员。随后几年，ITAA 和 TIA 也参与了 NSTAC 的活动。

除此之外，为了能随时解决国家安全和应急战备（NS/EP）系统中新风险，国家通信系统（NCS）负责运营着国家电信协调中心（NCC），该中心的人员既包括联邦政府的雇员，也有来自电信工业的人员。自从 1984 年成立以来，NCC 已经共享了很多电信事故方面的信息，以期在一个“极端危险”的环境中恢复长途通信。“极端危险”的概念现在已经扩大为包括对运行、行政管理、维护和供应等工作的电子入侵。为响应 PDD63，NCC 扩大了它的范围，涵盖了网络威胁，并通过电信工业信息共享和分析中心（NCC-ISAC）实现了对影响电信基础设施的大规模物理和网络入侵事件的信息的共享。电信 ISAC 信息共享的范围包括组织、人事、流程、设施等方面的信息。

IT 业也已对信息共享挑战采用了正式的应对措施。2001 年 1 月，国家中很多领先的高科技公司在网络空间安全问题上开始了合作，宣布组建一个新的 IT 信息共享和分析中心（IT-ISAC），其目标是要提高联网的信息系统的可用性、保密性和完整性。

### 互依赖性

国家基础设施所发生的深刻变革包括技术上的互依赖性、旧管制规定的撤销、对技术的极大依赖等，它们引起了对基础设施保障的新挑战。某些基础设施非常重要，以至于它们一旦损失某种能力或遭受破坏，将大大危及国防安全和经济安全。除信息与通信技术之外，没有哪种技术能够在这场巨大变化中担负更多的责任并深刻影响其他基础设施。

国家关键基础设施系统由公共和私营部门混合组成。因此，在有关安全、保护和经济竞争的问题上具有很复杂的多样性。私营业主在面对收入的损失和其客户、政府管理者、投资者和保险公司的信心的下降时，会努力恢复营业收入和客户的信心；对公共部门来说，为避免将来的攻击，政府会把重心集中在保护国家安全上，寻找和处罚攻击者。这种利益交叉的结果是任何的关键基础设施安全解决方案都需要政府和私营企业的一致协调。除此之外，还要在所有级别的政府实体中进行较好的协商，避免重复性的、不必要或不一致的要求。

1995 年 1 月，美国国家安全局局长就美国信息系统的威胁和安全需求向国家安全电信咨询委员会（NSTAC）发布了通告。作为回应，NSTAC 的负责人在 1995 年 3 月讨论了信息系统的威胁，并后来将这些回应文件转交给了克林顿总统。文件指出：

“政府和公众信息系统的完整性正日益处于遭受入侵和攻击的危险之中。国家的其他基础设施，例如财政、空中运输管制、电力等，也要依赖可靠的和安全的信息系统，并且也面临这样的危险”。

克林顿总统在 1995 年 7 月答复了 NSTAC 的这封信件：“欢迎 NSTAC 正在进行的这项通过与政府合作来制止对我们的国家信息和电信系统的威胁的工作。”克林顿总统要求 NSTAC 以“来自国家信息基础设施使用者的观点”评估国家安全和国家的快速发展对于信息基础设施应急战备状况的需求。

在提高关键基础设施保护问题的意识方面，NSTAC 担任了早期的领导角色。经过和政府的对话，NSTAC 确定了三类需要优先评估的关键基础设施：电力、金融服务和运输。特别是，

NSTAC 针对其信息系统调查了每个基础设施对信息技术的依赖状况和信息系统具有的相关信息保障风险。因为这些垂直的产业基础设施高度依赖 I&C 的解决方案，对每个基础设施进行的系统化评估也显示了 I&C 部门的准备状况。NSTAC 在 1997 年 3 月、12 月和 1999 年 6 月分别完成了对电力、金融服务和运输基础设施的风险评估。在每个评估中，它将相继的建议报送给了总统。尽管其中很多建议已经过时，但有些建议仍然有效，而且有些建议也可以被用在其他的关键基础设施上。

### 风险管理方法

I&C 部门认为需要采用多面方式来管理风险并改进美国在信息基础设施保障等问题上的合作。这种合作一定要跨越工业界并能促进工业界和政府走到一起。I&C 部门的风险管理要素包括意识、教育、培训、最佳实践措施、研究和开发、信息共享、重建和国际协调。

#### （1）意识和教育

总体而言，促进意识和教育是在 I&C 部门内的一项已经标准化的工作。本部门打算继续利用行业协会来开发并赞助教育和培训项目。意识和教育也被认为是推广工作的一部分。

I&C 部门协调机构正在实施一个面向国家决策者的推广项目，包括国会成员简报、早餐简报及参议院和众议院咨询，还包括国会听证会上的发言以及与白宫及其他的行政官员的一般会议。

#### （2）地方的参与

几个大的国家级审计和业务风险团体已展开了空前的合作，面向董事会、行政管理层和公共-私营机构首席审计官，以提高他们的安全意识和教育水平。这些团体包括内部审计师协会（IIA）、美国注册公共会计师协会（AICPA）、信息系统审计和控制协会（ISACA）和全美公司董事联合会（NACD）。

审计师和 CPA 联盟已在全国范围举行了 5 次地方会议。2000 年 4 月 18 日在华盛顿特区举行的会议具有广泛的参与性。联盟还开发了一份董事会指南，在会上进行了宣读。此外，2000 年 4~9 月的会议中，来自美国各地的审计师和董事都讨论了该指南。

会议参加者包括华尔街的分析人士以及“五大”公共审计公司和保险公司。地方性的商会也对各自地区的活动提供了支持。

#### （3）全球信息安全峰会和工业界联盟

全球信息安全峰会聚集了世界各地的工业和政府领袖。会议讨论了信息安全和基础设施保护问题。2000 年 10 月举行的第一届全球信息安全峰会加强了对安全问题的意识，促进了跨国和跨部门的合作，帮助了确定政策需求，突出展示了信息安全方面最好的实践和案例。除此之外，一系列高峰会达成了在信息安全问题上的全球合作意向。正如 1998 年 10 月在伦敦成功举办的国际“千年虫”计算机问题会议一样。那时，全球面临解决“千年虫”的挑战，均期待这次全球信息安全峰会能加强跨行业的合作，以便构建安全的全球经济环境。

#### （4）培训

信息与通信部门认为对信息安全专家的评估和培训是非常重要的，而且本部门正在努力就如何保护系统而对员工展开培训。从拒绝服务攻击中我们知道，一个系统的安全与人和技术都有关系。信息与通信部门制定的培训方法包括：对安全技巧集的研究，以便确定哪些是关键的信息安全技巧；在大学通过授课（或其他方式）传授上述技巧；推动更多的“大学优秀中心”的成立；为研究关键基础设施保护筹备资金。

找到合适的信息安全人员非常困难，这是因为这种人才需要不断的培训和教育。这种培训和教育远远超过了 IT 工作者通常所能够获得的培训和教育。很多涉及信息安全的职位需要美国国籍，特别是那些联邦政府中的职位，所以通过移民手段或外包给其他国家的想法一般不会被采纳。

#### （5）最佳实践措施

信息与通信部门有责任关键基础设施保护提供最佳实践措施。它正在很多垂直部门中寻求合作伙伴，以便加快这项工作。除此之外，信息与通信部门还负责和各级政府合作。例如，ITAA 已经与联邦政府的首席信息官委员会进行了合作，努力使各部门和机构的首席信息官能够共享业内最好的信息安全实践经验。同时，工业界正在获得由政府开发的最佳实践措施。2002 年 4 月，互联网安全联盟（ISAlliance<sup>SM</sup>）宣布了最佳实践措施和信息安全策略开发活动的路线图。ISAlliance 成立于 2001 年 4 月，它是在各基础设施部门和国际成员间交流工业需求和信息的工具，与卡内基·梅隆大学的软件工程学研究所（SEI）、CERT 协调中心（CERT/CC）、电子工业同盟（EIA）、联邦贸易协会努力合作。ISA 最佳实践措施工作小组正在致力于两类实践：策略实践和操作实践。在策略实践方面，同盟提交了关于安全意识与培训、安全策略、安全管理、安全政策和规则、业务连续性计划等白皮书。在操作实践方面，内容包括监听和审计、脆弱性管理、密码技术、事件管理等。

#### （6）研究与开发

信息与通信部门如果在研发方面不投入数十亿美元，美国就不能维持其产品和服务中所处的世界领先地位。然而，目前 I&C 部门在研发中还有很多差距。工业界的研发项目一般主要集中在能够出新产品的领域。政府（主要是国防部）投入到信息安全的研发的资金则主要用于解决国防和关键的安全问题上。我们相信，在没有市场力量和政府行政干预的情况下，工业市场驱动的研发项目和面向国防的研发项目之间的差别可能难以消除。

为了确定存在于整个信息与通信部门的研发差距，我们通过对一系列工作组的调研提交了研究与开发问题报告。主要的工作组包括 NSTAC 的研究与开发交流工作组和电信与信息安全工作组（TISW）。

#### （7）信息共享

由于威胁总在持续变化，信息与通信部门认识到需要有正式及非正式的信息共享机制。互联网服务提供商是非正式的信息共享的例子。因为这些公司需要提供商业性的网络接入能力，它们通常有大量的网络安全专家，于是这样的公司便扮演了虚拟的信息共享和分析中心的角色。它们可收集检测到的威胁信息和入侵信息，在过滤这些信息（即移走客户敏感的数据）后将这些信息与客户共享。

#### （8）标准化实体

TIA 保持了与 T1 委员会和咨询组在电信安全标准问题上的密切合作。除此之外，TIA 与 FCC 的网络可靠性委员会（NRC）、网络可靠性和互操作性委员会（NRIC）也保持着合作，就网络安全问题为美国国家标准化组织开发 CIP 标准。TIA 还定期与来自全世界其他标准开发组织（SDO）举行会议，在双方感兴趣的领域展开合作。这些会议被称为全球标准合作（GSC7）和 RAdio STandardization（RAST10）会议。2001 年 11 月，来自欧洲、美国、加拿大、韩国、澳洲和日本的标准组织在澳大利亚的悉尼通过了决议，表示对以下项目的合作很感兴趣：

- 开发下一代互联网体系结构和安全指南；



➤ 开发下一代互联网特别协议和应用程序接口。

由于下一代互联网的安全性是内建的，并且非常重要，它涉及很多领域和标准化组织，因此是一个重要的标准化领域。下一代网络的安全问题与很多方面是相互关联的，包括网络体系结构、服务质量、网络管理、移动性、网络计费和付款。

下一代互联网安全标准的设计面临的最重要的挑战之一是我们不能将网络看作有清楚接口的单个系统。下一代互联网安全的很多标准化工作必须基于应用程序接口的原理，只有这样，安全网络才能构建成功。

（9）对政府的推广

作为信息与通信部门的领导机构，为了促进和鼓励信息共享，NTIA 每月举办两次信息与通信部门工作组会议（CISWG）。CISWG 是由工业和政府代表组成的跨部门的团体，提供关于国内最好的实践措施和国际 CIP 双边和多边活动的信息。CISWG 的推广小组委员会扮演了促进工业团体参与信息安全讨论的角色，通过双边协商和多边谈判使私营部门的观点得到讨论。同时，NTIA 也将与部门协调机构紧密合作。

除此之外，NTIA 还与位于 Rocky Mountain Corridor 的 Cheyenne 军事基地进行了合作，帮助由 DoD 主办的脆弱性评估。NTIA-DoD 是 USG 领导机构的第一个联合风险机构，在 Rocky Mountain Corridor 项目的基础上成立，由 NTIA 和 Verizon 负责，夏威夷是这个模型的下一个要测试的地区。

（10）重建

通过系统冗余、业务连续性计划和应急战备来减缓风险，对于信息与通信部门来说不是什么新的方法。这类工作常由灾难恢复公司实施，如Sungard和Comdisco。服务的类型和程度是多种多样的。灾难恢复服务的基本思想是建立一系列冗余和备份，并能在紧急情况下通过远程工具访问数据。维护地理上分散的设施确保了受到单点攻击或自然灾害的公司的数据资产不被破坏。

当然，公司可以选择在远离它们物理位置的地方维护它们的专用网络和数据存储设备。拥有多个数据中心的大公司采用的便是这种方法。但是它们也可能选择签订适当的灾难恢复服务合同，以便对系统进行测试并降低风险。

然而不幸的事，很多公司在运行过程中没有采取合适的恢复服务。一个厂商估计，在 1993 世贸中心爆炸事件中，350 家企业中的 150 家遭到了破坏，直至一年之后它们破产。

（11）国际事务

无论工业界的态度如何，很多公司都已经意识到，必须将关键基础设施保障问题作为一个国际性的问题进行讨论。电子商务进一步促成了全球化的商业环境，美国必须在促进以业务为核心的关键基础设施保障日程上保持领先地位。因此，很多组织或者对这些要求进行了直接响应，或者对公司的使命进行了扩充，增加了对于关键基础设施保障问题的考虑。

### 3. 工业界与政府的角色

在信息与通信部门内建立关键基础设施保护角色时，必须意识到工业界要和各种正规和非正规的组织相合作，与政府一起保护国家的关键基础设施。所以，我们目前面临的一项挑战在于我们要理解哪些关键基础设施保护工作应该由工业界来领导，而哪些则需要政府更积极的参

与。本章主要讲述以下四方面内容：

- 定义合作联盟；
- 工业界的角色和责任；
- 政府的角色和责任；
- 法律和立法问题，包括《执法通信援助法》（CALEA）和《信息安全法》（FOIA）。

### 定义合作联盟

信息与通信部门由各类企业实体组成，有些实体是政府性质的，而有些则是私营的。为了保护国家基础设施，在国家策略的层面上定义角色和责任是一项富有挑战的任务。为取得在这一问题上的一致意见，制定基本的原则是完全必要的。

《信息系统保护国家计划》第1版作为首部关键基础设施保障框架定义了以下原则：

“政府无法独自保护国家关键基础设施。私营工业、州和地方政府直接拥有、有效控制或极大影响着大多数对我们国家的安全和经济富强至关重要的基础设施。”

报告进一步陈述了联邦政府的角色，包括：

- 实现相关的行动案例，促进私营部门的投入；
- 与私营部门共享威胁信息和矫正措施；
- 支持私营部门设计自己的防护项目；
- 促进私营部门实现自己的防护项目；
- 为私营部门顺利开展其保护项目而去除障碍（如信息共享）；
- 刺激相关研究与开发；
- 在必要时，作为国家保护工作的领导。

当时的那份计划还提出私营工业的角色包含以下方面：

- 保持强健和可靠的服务交付系统；
- 维护客户的信心；
- 确保在面对威胁和脆弱性时的系统完整性。

此外，《信息系统保护国家计划》还观察到这一活动要通过加强工业和政府的“合作联盟”来实施。合作联盟可被定义为“一种法律上的合作联盟，通常涉及拥有共同权力和责任的各方之间进行的密切合作”。

国家计划中还制定了以下的合作原则：

- 自愿性；
- 双方共同感兴趣，具有清晰、集中、充分定义的目标；
- 双方都有关键的实施能力和角色；
- 相互理解彼此的价值、期望、需求、关注点和各自的目标；
- 持续、经常地交流；
- 做好规划。

信息与通信部门在此基础上又提出了下面的规则：

- 政府必须能够描述出对私营部门的期望，如工业界对威胁的响应。
- 在信息与通信部门中要具体情况具体分析。不同级别的性能和对于危害的不同的抵抗力代表了不同的保护代价。

- 合作方必须制定有关规则，以促进彼此的理解和融合。
- 股东必须切实考虑不同公司的具体环境有所不同。
- 合作方必须制定管理规则以达到彼此的理解。
- 合作方必须在规则暂时取消时对特别条件有共同的理解。
- 在业务或技术情况发生变化时，双方必须能够一致地对合作联盟和项目再进行协商。
- 政府不应该通过立法机构强迫工业界违反其自己的意愿。

广泛宣传和体现这些原则对于促进政府和工业界更细致地理解这些原则是 very 有效的。在这一基础上的交互将达到一个新的高度，有很多组织的交流很接近于这些原则的运行方式。

### 解决方案的要点所在

关键基础设施保障办公室（CIAO）在为国家计划 1.0 版拟定的大纲中，提出了下面的政策示例：

“美国的这一政策应当是这样的：任何关键基础设施的运行所遭到的物理或网络破坏必须控制在历时短、频率低、可控、地域上可隔离以及对美国的国家安全、经济、重要的政府服务、公共健康和公共安全损害最小这样一个规模上。”

信息与通信部门完全认可上述政策，并认为这一期望值必须是可实现的。国家基础设施要达到能抵御任何攻击并不会发生故障的状态是不大可能的。但是，必须建立一种环境，实现合理的安全级别。

一个一致的解决方案以及对行动和目标的细节和目的的定义必须由多个组织制定。工业界可接受的风险级别各不相同，例如，信息与通信部门能够接受的入侵级别比银行与金融部门高。而更高安全级别意味着更大的努力、更多的支出。鉴于这些原因，每个关键基础设施部门的工作细节都必须是特定的，但要遵循共同的基本原理。

### 工业界的角色

工业界的一个基本角色是确保私营企业提供合理、成本有效的安全性和可靠性。在部门级，要不断地推行意识培养和教育、最佳实践措施、推广、应用性研发以及信息共享项目。

工业界的另一个主要角色是定期评估部门及的脆弱性和风险，该过程中可以沿用与前几年国家电信咨询委员会（NSTAC）使用的相同或近似的方法。这些评估不但应考虑信息与通信部门，还要考虑到其他基础设施部门信息技术和通信问题。

### 政府的角色

除了合作联盟外，联邦政府还有一套能够单独实施的角色和责任。例如，政府应给关键基础设施保障工作提供实际有效的领导权，并能帮助提高国家对网络攻击及预防措施的意识级别。政府的责任分国内和国际两部分。美国在全球范围内要主导防御和贸易关系。这条链上的任何中断都会导致级联影响。因此，美国政府的职责是接受其全球关键基础设施保障角色，并就威胁的性质及如何响应威胁对外国政府进行教育。工业界要和多国组织和 NGO 互相合作，推动上述过程。

联邦政府的其他角色还包括：

- 在政府所有机构之间协调关键基础设施保障策略。作为政府的“千年虫”防御

“czar”<sup>①</sup>，John Koskinen 曾令人尊敬地完成了这一角色。国土安全办公室和关键基础设施保护委员会必须与工业界密切合作，提高关键基础设施保障的重要性。

- 联邦各机构应该采用强有力的关键基础设施的保障措施。这意味着，必须打击黑客对政府网站和其他信息资产的渗透能力。联邦政府将致力于和私营部门的密切合作，以保护关键基础设施。这种合作的方式主要以双向地交换入侵信息、病毒信息和其他事件信息为主。只要大家都有实现这一目标愿望，则必然会推动工业界的 ISAC、FBI 的国家基础设施保护中心以及其他组织的工作。
- 要开展 Internet 安全方面的前瞻性研究。Internet 自身和很多相关的革新都是联邦资助的研究项目的成果。通过资助 Internet 安全研究，联邦政府同样可以起到关键作用。
- 要对联邦各机构的安全工作提供资金，以实现足够的保障级别。应要求联邦各机构改进它们的信息安全处理过程并培训其人员，可是如果没有资金的话，这些工作的收效不会比口头演说好到哪儿去。

## 法律问题

### (1) CALEA 的经验和教训

公共政策和有效的关键信息保障有着密切而复杂的联系。由于政府和工业界正努力建立一种平衡的合作联盟，法规不能成为合作的障碍，不能导致不当的负担或者财政问题，也不能只使一方受益。如果在合作中缺乏可信和主动性，则联邦行政部门与工业界建立的合作联盟终将一无所获。

《执法通信援助法》(CALEA)就是一例。在 20 世纪 90 年代早期，执法领域和电信工业界在引进高成本的新型网络监督设备问题上产生了争执。CALEA 的出现打破了这一僵局，要求工业界开发能力标准，并授予了联邦通信委员会(FCC)的监督权。

### (2) 工业界和政府之间实施信息共享时的法律障碍

有很多公共政策因素阻碍了关键基础设施保障工作。公共部门和私营部门之间以及私营部门内部的信息共享对于一个国家的基础设施保障是至关重要的。但直到信息共享的法律和经济障碍被去除，合理的信息共享才能做到。

信息共享的障碍与《信息自由法》(FOIA)有关。

政府机构离不开计算机攻击的详细数据，以便更好地执法、实施早期检测并在政府和工业界内推动最佳实践措施的实现。然而，如今企业咨询专家却建议他们的客户不要主动与政府机构去共享计算机攻击的细节，因为这样会带来负面影响。他们认为，这些数据可能最终会在《信息自由法》(FOIA)的要求下被公开，即使政府机构不愿意这样做，这样的风险显然是不能接受的。

美国众议院和参议院中一些正在讨论的提案有希望能够通过保护这类信息而改善这种情况。这些提案提出了有限使用保护原则，这样提交给政府的关键基础设施信息便不会使信息的提交者蒙受损失。

---

① 意为“沙皇”，指在某领域具有决定权、领导权的政府人士。——译者注

## 4. 展望

### 趋势

I&C 部门中的执行层认为，在不远的将来，他们将能够真正位于一个数字世界中，通过 Internet 技术提供数字化的功能。Internet 协议将与人们的生活密不可分。手持设备的数量将在 2003 年超过个人计算机的数量。

但 Internet 上的语音服务和传输必须考虑安全问题。未来的网络入侵也将危害实时传输的网络语音数据。

宽带技术也给基础设施保障带来了新的挑战。时刻在线的调制解调器或 DSL 对数以千计的计算机构成了安全威胁。攻击工具将增加找到脆弱性机制的速度，而且寻找脆弱性看来似乎愈加容易。宽带技术在给家庭生活和业务运行带来巨大便利的同时也将带来更大的被攻击的可能性。

所有公司的董事会和决策层都应考虑 Internet 的安全措施问题。在此之前，信息安全问题无法获得应有的充分重视和充足的投资，这种情况应改善。在政府领导未能充分意识到必须通过教育和技术及管理流程的投资途径来解决信息安全问题之前，我们仍将面临巨大的威胁。

### 总结

I&C 部门今后在信息安全方面应该遵循一些基本的原则，包括：

- 维持工业界在制定和开发信息安全标准、实践措施和解决方案中的领导地位。
- 工业界进行自律非常关键。这将保障本部门的行动能够满足市场的检验和消费者的需求，风险面前保持积极和灵活的措施，并可确保所提出的解决方案体现了对于基础设施保障的正确理解。

具体建议包括：

- 扩大信息共享的机会。
- 增进对于关键基础设施威胁和防御的意识。
- 增加在网络空间安全方面的资金投入。
- 增加对位于网络空间防御前线的人员的培训与教育。
- 为确保关键基础设施对于网络攻击具有抵抗力，建立响应、资产恢复和工作流程。
- 进行国际协调，增强对于计算机犯罪行为的调查和惩治力度。

I&C 部门的协调员非常高兴有机会制定这份计划并能为增强基础设施保护意识做出贡献。参与制定本计划的成员欢迎对本文提出的任何问题进行讨论，并期望和各方在未来加强合作，共同制定关键基础设施保护和网络空间安全的国家战略。

---

## 十二、高等教育对保护网络空间的国家战略的贡献（摘要）

美国高等教育部

2002 年 7 月

---



扫二维码阅读全文

## 执行摘要

高等教育部门在美国的网络安全保护工作中发挥着重要作用。它的核心使命是为国家的未来培养了领导、创新和科技人才，它的科研项目成为很多新知识和由此而问世的新技术的发源地。此外，作为机构实体的大专院校还运行着世界上最大规模的计算机群和高速网络。

总之，高等教育是我国一大重要资源，可用来为网络安全开发解决方案和制定战略规划。它是一个充满科技活力的综合体，需要并且能够接触广泛的信息，同时也需要并且能够实现灵活高速的通信。高等教育的开放性创新价值最终体现为我们国的开放性创新价值。在很多情况下，高等教育部门的计算机和网络代表着未来的新兴系统。高等教育部门成功的安全保护可以为整个国家树立榜样。

美国的高教部门是一个大型综合体，作为其成分的院校和系统在范围、规模、使命和技术能力方面各不相同，差异很大，通过各种协会构成了松散的组织体系。其中的几个协会，包括 EDUCAUSE 和 Internet2，直接致力于院校级信息技术（IT）的研发。高等教育各大全国性协会还组成了高等教育信息技术联盟（HEITA）之类的联合会组织，旨在从行政管理的层次上协调各自的 IT 政策。

当今，大多数院校的教学使命要求每个学生都具有使用计算机和访问互联网的能力。学生的频繁流动、技术的不断发展、技术类别的多种多样、管理权力的分散下放、资金的短缺以及所涉人口的急剧增加，这些问题对院校“有线”和“无线”网络的安全提出了特殊挑战。高等教育的科研使命是国家创新的关键所在，而其推广服务的复杂性堪与电子政务方案的复杂性比肩。

尽管高教界复杂多样，但是它的基本价值观却是始终不变的，如知识自由和管理权分散等，这样的价值观高度重视专业人员的权利和责任。这些坚定信念对院校以何种网络安全保护措施取得成功有着重要影响，而且任何成功的网络安全保护战略都必定要考虑这些因素。但归根结底，安全是保护学术文化的关键。

高教部门的网络安全关键问题在两个层面上存在着很大差异：各个学校之间以及同一所学校的不同系之间。适于使所有问题都迎刃而解的方案是不存在的。虽然很多问题在其他工业部门也存在，但有不少问题在高教部门显得更加突出。

EDUCAUSE 就高教部门有哪些问题应在《保护网络空间的国家战略》中得到强调组织了一次网上调查，调查结果将有助于战略措施的制定。与其他经济部门的相似性和不同点在调查结果中均有体现，从而有助于强调增强信息共享和寻找最佳实践措施的重要性。

高教部门全国性组织领导人签署了一项包含 5 部分内容的“网络安全行动框架”，将由国家科学基金会（NSF）出资召开 4 次系列会议，以此调动整个高教界全部投入到制定一项全面的国家战略的工作中来。

概括而言，高等教育在美国的网络安全保护工作中发挥着重要作用。它正在组织力量研究和解决整个国家都面临的网络安全问题并且得到了其最高领导层认可，已经就传统和创新性解决方案与联邦政府和其他工业部门进行了卓有成效的合作。

## 1. 介绍

如今已被视为国家基础设施关键组成部分的互联网信息与通信资源是科研和教育不可或

缺的工具。每天有 90% 的学生和教师访问互联网。自由公开的信息交流是学术事业的灵魂，同时也是美国大专院校履行其教育和科研职责所必不可少的媒介。

国家应对恐怖主义威胁的措施必须包含加强和保护大专院校网络和信息资源安全的步骤。此外，高教部门也有责任确保他们的计算机和网络设施不会被人用来攻击校园内外的关键基础设施。我们在对网络安全新需要做出反应的同时，还必须对具体行动做出周密评价，在这些需要与作为学术价值核心的自由和公开的基本保障之间找到平衡点。

高教部门是可用来在一个开放自由的社会里开发网络安全解决方案和制定网络安全战略的一大国家资源。高等教育的价值最终会体现为对国家的贡献。在很多情况下，高教部门的计算机和网络代表着未来的新系统。高等教育部门成功的安全保护可以为整个国家树立榜样。

## 2. 高教部门的网络安全工作

长期以来，网络安全问题一直深受院校、系统和协会的密切关注，雇用安全人员追踪和打击入侵行为、召开地区性专业开发和信息共享会议、不断改进应对新程度新类型威胁的政策之类的现象都有力地证明了这点。麻省理工学院、密歇根大学、华盛顿大学、卡内基·梅隆大学、印第安纳大学等学府是开发安全技术、政策和方法的先驱，这些技术、政策和方法如今已经广泛应用到商业领域中。

最近，高教部门在全国范围内推动网络安全发展方面实施了一系列意义重大的措施。相关的研讨和规划工作是由组建于 2000 年夏天的 EDUCAUSE/Internet2 计算机和网络安全工作组实施的。2002 年年初，工作组起草了一份包含 5 部分内容的“网络安全行动框架”，致力于：

- (1) 使 IT 安全在高教部门得到更高和更切实际的重视；
- (2) 运用现有安全工具更好地完成工作，其中包括修订制度性政策；
- (3) 为未来的科研和教育网络设计、开发和应用安全保护手段；
- (4) 增进高教部门与工业界和政府之间在安全保护方面的合作；
- (5) 将高教部门的安全保护工作与范围更广的全国性加强关键基础设施保护的工作融合为一体。

该“行动框架”于 2002 年 4 月得到美国教育联合会和高等教育信息技术联盟与会成员批准，并由网络空间安全总统特别顾问 Richard Clarker 于大专院校信息技术领导人国家政策年会“2002 年网络会议”上正式对外公布。工作组目前正在制定召开由国家科学基金会出资的 4 次系列会议的计划，旨在为改善高教部门网络安全状况制定出更详细的战略，其中包括各类院校的最佳实践措施和网络安全行动指南。我们只要仔细分析一下美国高教部门的特点，便不难意识到，这一过程会遇到哪些挑战。

## 3. 美国高教部门人口统计

高等教育是游离于美国经济之外的一个部门。各院校尽管有很多共同的特征和目标，但是在类型、规模、使命、资源和复杂性方面存在着巨大差异。保护网络空间战略的大部分内容适用于所有院校，但同时也有部分内容可能只适用于某些特定院校。最理想的战略应是放之四海而皆准的。



美国的高等教育部门由 11 000 多个专科以上教育机构组成。本报告阐述的战略主要针对美国高等教育系统内 4 048 所被确认具有授予学位证书资格的院校，这些院校总共吸收了 1 450 万学生（包括研究生和本科生），雇用了 300 万教师，总体预算接近 2 000 亿美元。

尽管只有 42%（或 1681 所）院校是公立学校，但是它们吸收了 76% 的学生。公立和私立院校由于多种原因而存在明显区别，其中包括管理结构、法定责任和筹资方式方面的差异。公立院校的资金来源主要是州政府，往往有责任对特定地区的公众提供服务。很多公立院校被视为州政府的下属机构，需要服从州政府在管理和政治上的很多考虑。大多数州都建立了高等教育系统，将若干所院校连接为一个整体，由一个合作管理委员会负责各院校间的协调。由于存在着复杂的多样性，没有一种模型能够涵盖美国专科以上公立院校的全部情况。

在这 4 048 所院校中，有 40% 以上是两年制学院。这些基于社区的学院尽管与别的学校在学生数量上十分接近，但是它们服务的学生人口在需求方面与传统的四年制寄宿大学或学院有着很大差别。它们注重职业技能的教育取向为美国技术劳动力队伍的很多成员提供了进入经济领域的机会，其中自然也少不了为计算机安全职业培养人才。

其余的 2 267 所学校是有资格颁发学士学位的四年制院校。其中一半以上可以授予硕士学位，488 所（或 20%）可以授予博士学位。在校就读的学生规模从不到 200 人至 4 万人以上，差异很大；但大多数院校的学生人口在 1 万~2 万之间。学校应用的技术也各不相同，在小规模文科学院，计算机主机主要用于行政管理和图书馆服务；而在有科研性质的大型大学，所配备的超级计算机和先进网络主要用于开发尖端科学和工程。

在 4 048 所院校中，有 140 所参与了由政府投资的重大研发工作。联邦政府平均每年对大学科研项目投资 160 亿美元，其中给 Johns Hopkins 大学的投资就多达 7.7 亿美元。这些科研项目全都高度应用网络技术，有很多甚至是直接开发未来的计算机和网络技术的。

## 4. 美国高教部门的组织

美国高教部门由各种大专院校和不存在等级关系的院校协会组成。很多院校是美国教育联合会（ACE）的直接或间接成员，美国大学协会（AAU）、州立大学和政府赠地学院全国协会（NASULGC）、美国州立学院和大学协会（AASCU）、独立学院和大学全国协会（NAICU）和美国社区学院协会（AACC）等专业组织的主席是它们在联合会中的代表。一所大学或学院可能同时是其中若干个协会的成员。

各校计算机和网络最高负责人首席信息官以及其他很多 IT 专业人员加入了 EDUCAUSE，这是致力于院校计算机和网络各方面工作的一个协会组织。很多科研性院校还是 Internet2 的成员，该组织侧重于尖端网络技术的科研和教育。界内还有很多协会以包括计算机安全在内的各自的专业取向或学科和科研重点对院校的行政管理者 and 教师提供支持。

近年来，高教部门的几个主要协会联手组建了高等教育信息技术联盟（HEITA），旨在就高教部门 IT 政策问题取得一致意见。该联盟最近签署了前文提到过的“网络安全行动框架”。HEITA 的成员包括：

- 美国社区学院协会；
- 美国州立学院和大学协会；
- 美国教育联合会；

- 美国大学协会；
- 科研图书馆协会；
- EDUCAUSE；
- Internet2；
- 学院和大学商务官员全国协会；
- 独立学院和大学全国协会；
- 州立大学和政府赠地学院全国协会；
- 大学成人教育协会。

## 5. 网络安全与高等教育的使命

美国的学院和大学在教育、科研和推广服务三大基本使命方面存在着对网络和计算机的相同需求。

### 教育

从前文所述的人口统计中可以看出，高等教育部门由各种大专院校组成，其中从注重具体专业的学校，到其活动范围和运行复杂性堪与城市相比的综合性多学科大学，差异很大。不过，教学是所有院校最基本的工作内容。

教育越来越不被视为由老师向学生传输静态知识，而演变成学习者在老师的指导和鼓励下，通过与其他学习者合作，提出自己的看法、实践原理和技能以及解决问题的复杂互动过程。这种教学方法依赖于各类信息的便于获得，以及对学生与学生之间、学生与教师之间及与世界各地其他人之间的交流和合作的强有力支持。

以学习者为中心的主动教育方式是普通民众全面参与被网络连接得越来越紧密的社会的关键所在，也只有近来通过互联网、环球网、数字图书馆、电子邮件、线索讨论和相关技术的发展才能实现。获取这些技术和工具至关重要，而且也不再是一种奢望。这也是为什么“网上校园”如雨后春笋般出现的原因，目的就是要让每个学生都有直接接触计算机和互联网的机会。

与此同时，大专院校的人口构成也发生了变化，越来越多的学生不必再有传统背景，越来越多的学生超过了 18~22 岁年龄段。这些趋势大大刺激了对基于互联网的解决方案的规划和投资，使很多院校将支持性项目和教学资源转而投放到网络上。而根本原因是，教学核心使命使校园内每个人都产生了直接接触互联网和其他 IT 资源的需要。

当然，高等教育还在培养网络安全专家方面发挥了主要作用，这些人才有的应聘在其他部门负责基础设施的保护工作，有的则从事未来安全方法和技术的开发研究。网络安全专业的支持和发展将是制定行之有效的网络安全国家战略的关键。

### 科研

尽管高教部门中直接参与政府出资科研项目的院校相对较少，但是人们已经认识到，使现代大学具有科研性质，是当今开发新知识、新方法和新技术以及培养新学者和技能娴熟专业人员的最佳途径。主要在大专院校开展的基础理论研究为将来的实际应用和经济发展播下了种子。过去几十年里，高教部门给计算机和网络领域带来了累累硕果。

近年来，越来越多的学科人士意识到，生产性科研需要直接使用在极高速网络上运行的超级计算机。在联邦研究机构帮助下，高教部门已经一步步迎接挑战，开始实施“高级计算基础设施联盟”、Internet2、网格计算等大规模网络和计算项目。高等教育机构如今支持着世界上大部分最大规模的计算机群，并且维持着与世界各地同行的高速连接。事实上，互联网上登出的网址约有15%是科研教育界的。

### 推广

目前，很多大专院校积极开展推广项目，即与专业相关的业界合作，将学校的知识和技能运用到实际工作之中。推广同时也是教学和科研过程中信息、经验和服务的双向交流。推广服务的成功关键是信息在校内外参与者之间的通畅流动。院校的这部分活动已经把互联网作为提高效率的手段。将来，网络对推广活动的高质量支持将给电子政务方案带来同样的机遇和挑战。

## 6. 网络安全与高等教育的价值体现

尽管大专院校的任务复杂多样、各不相同，但它们在几条基本原则上是高度一致的：学术和知识自由、个人责任、多样化和多元文化。要想开发出成功的方法确保高教部门网络的安全，就必须考虑这些基本原则。

学术自由在高等教育领域有着公认的悠久历史，这是在新知识的发展过程中确保质疑、辩论和追求得以顺利进行的权利和责任。这种历史与图书馆界提倡的知识自由和宪法保障的言论自由密切相关。学术自由在美国得到广泛支持，它不仅仅是一种权利，同时也是对创新和发明的一种基本要求，而正是创新和发明使我们这个国家变得越来越强大。

高教部门的机构基本上不支持那种用组织系统表控制日常事务的自上而下管理文化。大多数院校更像是权力分散的专业组织集合体。很多教师（和越来越多的学生和工作人员）以民主方式参与学校管理。教师个人维护自己的自主权，将其视为创新和发明不可或缺的要素。完整的学术体系、行为的规范和校方制定的政策构成了学生和教师都要遵守的标准。

学生数通常在校园人口中占最大比例。尽管教学的核心使命要求为所有学生访问校园网和互联网提供方便，但是学生使用高科技的目的与教职员工是大不相同的。住宿学校所面临的一大独特挑战，就是要认识到学生使用网络主要是为了娱乐，而教职员工则往往出于学术或业务目的使用网络。

校内大多数人都强烈反对不合理地限制使用网络和计算机。从某种角度说，这属于技术方面的争议。而我们的信息经济中诞生的全新部门就是起源于独一无二的校园环境的，它提供了新经济所需的全部人才，其中从总统到在校学生，堪称应有尽有；同时还为通过强大网络探索新理念和设计提供了无数机会。国家研究理事会最近进行的一项研究有力地支持了这样的结论：互联网和校园网的开放性质始终是创新应用快速和灵活发展的一大重要因素。

从另一个角度看，抵制规章制度可能是个人工作重点的一种含蓄反映。例如，从事课题研究的教师和他们的研究生往往会把注意力集中在“自己的实验”上，而不去理会计算机系统管理上有什么规定。他们虽然非常重视自己工作的知识产权保护，但常常要到入侵事件发生之后才会意识到网络安全问题与他们有关。由于科研资金的使用以及管理（包括用于科研目的的计算机的使用）的权力是下放给教师或实验室的，所以很多安全问题在以往并没有得到足够的重

视。但是如今，这方面的问题已经引起了密切关注。

所有这一切并不是说明在大专院校无法确保网络安全。相反，行之有效的解决方案借助各校实现自身目标的各种手段，必定能在这种文化氛围下发挥作用。每所学校都必须考虑的一项重要活动是对学术价值的与网络安全之间的相互影响展开公开讨论。归根结底，网络安全是保护学术价值的关键条件。实施于高等教育环境的解决方案对于整个国家都至关重要，因为开放和创新的价值对于整个国家都是相同的。

## 7. 高教部门的计算机和网络基础设施

任何改善院校网络安全状况的计划，都必须考虑所涉计算机系统和网络的类型和配置以及解决方案所需动用的人力和其他资源。这些因素因学校而异，存在很大差别。单个校园网络的联机系统千变万化，有的可能是用于国际课题研究的超级计算机群，有的可能是用于给员工发放工资的主机，有的可能是学生自有的便携式计算机。

在校学生的数量也会带来不同结果。为有 3 万学生的大学设计的解决方案很可能在规模上大大超过小型文科学院。同样，小规模学院遇到的管理问题，到了配备有充足高速计算能力的综合大学，会成比例大幅度放大。以下是依学校规模和可用资源的不同而不同程度存在的安全问题：

- 校园网如何连上互联网？小规模学院可能会通过某一商业互联网服务供应商或从地区性大学网络获得与互联网的连接，基本安全服务和其他种类技术支持可能也均由对方负责。另外，大规模科研性院校则可能拥有多重互联网连接，这既是为了冗余备份，同时也是为了便于与 Internet2 或其他尖端网络连接。
- 校内人员需要掌握多高程度的专业技术知识？学校可以在多大程度上评价和使用各种现成的解决方案并对所选择的方案提出具体要求？从学校以外可以得到多大程度的帮助？
- 学校的中心控制有多大能力？在计算机和网络高度密集的学校，解决方案通常侧重于边界和连接部位（即实施中心控制的部位），而较少注意单个计算机和局部网络。中心控制的问题也与学校的政策和纪律制度密切相关。在一些学校，仅仅通过制定适宜政策就能在很大程度上实现控制；而在其他学校，侧重具体的技术限制会显得更加重要。

学校内的技术多样性也对安全提出了挑战。以下是与各种不同系统相关的问题：

- 如何将校园网络划分成不同区段（或许是物理上的，但最可能是虚拟的），以使各种系统和网络都能达到适宜的安全级别？有了恰当的分段，学校的管理系统没有理由不像私营部门的系统一样安全可靠。
- 如何将学生的自有计算机连接到校园网上？在非寄宿学院，学生通常是通过调制解调器或商业互联网服务供应商与校园网相连的。而在寄宿学校的学生宿舍，学生的自有计算机往往跟管理、科研和教学系统一样，是直接连接到网络上的。学生的自有计算机轻易就能形成使用学校资源的最大计算机群，但同时，它们也是最难实现标准化控制的计算机。
- 校内配备了哪些特殊用途系统？例如，医疗系统具有提示与生死相关的信息和满足

《健康保险可携带性和责任法》（HIPAA）规定的特定法律要求的功能。这样的系统几乎全都是需要特殊的安全解决方案的。

最后，在考虑哪些类计算机系统和网络需要确保安全时，以下几个问题在各种大专院校中普遍存在：

- 预算紧张，加强安全的很多益处往往被认为不会给学校本身带来什么直接回报。
- 大学与其他工业部门一样，深受供应商产品安全缺陷之苦。由于高教部门的计算机和使用者复杂多样，这些缺陷对高教部门的影响常常不成比例。
- 科技在不断进步，每项新技术的问世都会带来新的安全问题。例如，最近流行的无线连接产生了数据（包括口令）暴露的新问题。随着掌上装置的日渐普及以及掌上装置与移动电话结合用于普通通信用途，今天行之有效的安全解决方案可能很快就会变得无法适应。

## 8. 回应有关国家战略的问题

作为实施“网络安全行动框架”准备工作的一部分，EDUCAUSE 就白宫关键基础设施保护委员会提出的 53 个“亟待解决的问题”，在高教部门进行了一次网上调查。各成员学校应邀到 EDUCAUSE 网站上对高教部门特别关注的 3 个问题做出回答，同时也被要求在其他地方阅读或回答调查表提出的所有问题。这一要求在 EDUCAUSE、Internet2 以及高等教育信息技术联盟等协会组织的成员中间广泛传播。这次有关国家战略问题的调查结果将对“行动框架”的实施起到至关重要的作用。

EDUCAUSE 大约收到 100 份答卷并据此制成了表格。调查结果显示，界内人士普遍认为高教部门的网络基础设施运作与其他经济部门或政府机构的网络基础设施运作非常类似。很多答卷指出，用于学生宿舍的宽带 ISP、服务于学校管理系统的公司信息和交易中心以及用于科研和教学目的并高度分散的各系和各实验室局域网，几乎涵盖了校园网的所有特性。因此，关键性的行动之一，是针对高教部门如此纷杂的情况就网络安全问题开发和制定最佳技术、政策和操作手段。行动过程中还可以考虑到教育界以外的类似系统中寻找解决方案。

其他答卷内容概述如下：

- 预防从校外发起的攻击；
- 预防从校内发起的攻击；
- 组织和协调。

### 预防从校外发起的攻击

如何在预防大学大规模计算能力因拒绝服务攻击和针对其他网站的恶意行为而遭破坏的同时保障学术自由？

所有应答者都非常关注把握知识自由、隐私权和安全之间平衡的需要。与此观点相一致，美国大学教授声援电子通信学术自由协会（AAUPSAFEC），<http://www.aaup.org/statements/SpchState/Statelec.htm> 认为，不会对科研工作形成阻碍的合理的计算机安全措施通常也不会约束学术自由。提供适度的安全措施是有力保障隐私和自由权利的前提。

应答者认为，要想达到这种平衡，就需要从行政管理、用户及技术三个层面采取措施。在

行政管理方面，工作人员必须制定和执行一项适应特定环境的技术政策。政策应该建立在度量统计的基础上，设置有最低要求，对于收集和利用来自其他来源的与安全问题相关的数据有推动作用。

应制定一项用户教育计划并坚持加以实施，侧重于加强用户对安全破坏者的了解，而不仅限于以改变系统或网络的方式来应对攻击。通过教育应该使用户对自己在维护网络安全方面能够发挥什么作用、应恪守哪些网络安全规则以及错误操作会带来什么不良后果有一个清醒的认识。

在技术方面，应该定时对照 SANS/FBI TOP 20 列表 (<http://www.sans.org/top20.htm>) 以及有关已知脆弱性的类似来源对系统进行检查。操作系统软件应该通过已知的最新补丁和供应商的安全解决方案及时更新。建议的安全技术包括精选配置的防火墙、入侵检测系统、防病毒软件、安全的文件传输协议(FTP)、电子邮件病毒过滤软件、个人防火墙软件、配置和安全协议、强劲口令、脆弱性扫描、公钥基础设施和数字签名。除了规避脆弱性以外，高教部门还应积极参与用于检测和减少拒绝服务和相关攻击的新技术的研究、开发和试验工作。

### 预防从校内发起的攻击

大学系统的哪些功能和应用需要高水平的 IT 安全保障（如医疗档案、学生档案、科研实验、专利等）？在当前学术环境下如何最大程度地发挥安全保护的作用？

对于这两个问题，应答者一致指出，应从行政管理层面建立一个安全体系，用以确定所需要的保护级别以及制定和采用适宜的政策和技术。每所学校至少运行三种不同类型的网络（科研网、商业用途网和互联网服务供应商提供的网络）。保护图书馆电子信息资源的工作可能与保护处理个人信息和金融交易的商业系统的工作有很大差别。相关规定已经包含了有关《健康保险可携带性和责任法》(HIPAA)、《家庭教育权和隐私权法》(FERPA) 以及各种州法律和法规的要求，基本不需要增加联邦或州级别的法规。

### 组织和协调

各校应该如何以最佳方式组织起来以解决他们经常遇到的 IT 安全问题？应在全国范围内形成公认的最佳实践方式或标准吗？应在各校首席信息官(CIO)和系统管理员之间建立有关威胁和脆弱性的信息共享机制吗？

调查结果显示，参与网络安全工作的各实体之间需要加强信息沟通，正如计算机科学和电信委员会(CSTB)最近的一份报告所建议的那样，需要就有关基础设施安全的信息创建一个信息交流中心，其中涉及从州政府到工业界和联邦政府级别的信息和资源。目前已经建立了很多信息交流机制（如 SANS、UNISOG、CERT、InfraGard 等），然而在高教部门内部疏通和加强信息交流会带来很多益处，这样可以为高教界提供重点更为突出的信息源。EDUCAUSE 被认为是帮助组织和协调这方面工作的合适机构。此外，各院校还应任命一个首席安全官，负责保存资源、监督本地操作和作为代表参加全国性对话。需要再次强调的是，不仅仅是信息交流，政府在其他方面的疏忽也应该降至最低程度。

## 9. 网络安全行动框架

加强高教部门信息技术系统和资源安全所必不可少的“网络安全行动框架”将作为协调院校层面乃至国家层面各种活动的基础。该“行动框架”已经通过美国教育联合会和高等教育信

息技术联盟会得到本部门高层领导的正式批准，内容涉及以下五个方面。

### **使 IT 安全在高教部门得到更高和更切实际的重视**

对于高教部门管理者来说，校园计算机和网络的安全，特别是物理安全，已不再是一种新的责任。“9·11”事件的发生使系统中以往没有得到充分重视的脆弱性突出显露出来。面对技术和管理资源的无数竞争需求，很多学校无力摆脱它们在科研和教学方面对安全可靠系统越来越强烈的依赖。因此，安全状况的改善，在很大程度上取决于如何提高管理层对校园 IT 安全计划的重视，其中包括院校的最高行政领导。

### **运用现有安全工具更好地完成工作，其中包括修订制度性政策**

安全涉及计算机、网络及其使用的每个方面。众所周知，现有系统非常脆弱，这已经被网络蠕虫和拒绝服务攻击近来造成的破坏所充分证实。虽然很多攻击得逞的原因是计算机操作系统和应用软件的缺陷，但是很多情况表明，系统遭到破坏是由于使用者忽略了系统开发者已在系统中提供的根本性保护措施。因此，对于每个负责计算机、信息服务器、网络成分和校园 IT 基础设施其他部分的人员来说，第一要则就是要始终使系统处于供应商支持的最新安全水平。

此外，现行政策中涉及安全的个人、管理和部门责任的说明有很多已经过时，不再适应当前的情况。这些政策内容也需要不断更新才能确保对安全责任的普遍预期得到满足和实现。

### **为未来的科研和教育网络设计、开发和应用安全保护手段**

学术网络面临的重大挑战之一，是如何促使网络功能的改善以及其他形式的创新持续保持流动，以使整个高教部门都能接触到最出色的信息技术工具，支持科研和教学目标的实现。从某些方面说，无论是目前还是将来的网络，安全状况的改善与功能开发目标是相抵触的。当功能和没有作为同样重要的因素而被考虑到最初的网络设计中的时候，就像当前通常的做法那样，情况尤其如此。

我们必须付出巨大努力，使新开发出来的网络既功能先进又安全可靠。结构体系的平衡点必须反复验证，相关的试验必须进行，研究成果必须广泛传送给网络开发商和制造商。

### **增进高教部门与工业界和政府之间在安全保护方面的合作**

历史上，网络，尤其是互联网的设计、开发和应用都是政府研究机构、大学研究人员和计算机业公司之间合作努力的结果。要想明显改善网络的安全状况，就必须不断在研究、开发和技术转让诸方面加强协调合作。联邦政府为网络安全研究新投入的资金必须流向负责研发工作的机构，而这些机构必须努力确保研究成果尽早投入使用。

### **将高教部门的安全保护与范围更广的全国性加强关键基础设施保护的工作融合为一体**

“9·11”事件以后，联邦、州和地方政府为了应对潜在的恐怖主义攻击，特别是针对关键基础设施的袭击，迅速采取了改善安全状况的行动。高教部门的网络和 IT 资源是国家基础设施的重要组成部分，高教部门的行动必须与负责国家稳定和社会安全的机构高度协调一致。

## **10. 下一步行动**

“行动框架”确定了高教部门提高信息技术安全所必需的全面行动步骤。此外，上文概述的调查问卷初步结果中包括有待研究的问题，都将在高教部门内以及全国性的一系列活动中得

到进一步的分析阐述。

### 通过 NSF 出资召开的会议制定高等教育安全战略

为了产生重大转变和确保最大范围和最高层次的参与，高教部门正在规划接下来几个月的一系列补充工作。提高界内人士安全意识和制定具体安全战略是国家科学基金会出资于今年下半年召开的四次系列会议的主要工作目标，高教部门的重要利益相关人都将参加这些会议。

### 外派的工作任务和研究项目

EDUCAUSE/Internet2 计算机和网络安全工作组还将委托外界专业人员承担法律问题和风险管理、IT 安全计划和政策分析、IT 安全组织模式介绍、计算机安全风险分析模型和模板设计、突发安全事件分析等重要课题的研究工作。虽然整个高教部门都会对最佳实践方式的开发提供道义上的支持，但是忙于化解当前危机的安全专业人员却几乎抽不出时间来研究问题和验证解决方案。外派研究项目最终形成论文、报告和情况分析文章，对于确定问题和满足高教部门专业开发需要也是至关重要的。这些结果也将在领导人会议上分发给与会者，经修改后还将集结发布以更广泛地散发。

在努力促使整个部门广泛参与的过程中，工作组将继续为本部门开展推广服务工作。为高教部门制定一项战略将是一个需要广泛讨论、反复修改和不断更新内容的渐进过程。

### 确定最佳实践方式和共享通用解决方案

高教部门有共享信息的传统，这种传统对于提高院校计算机和网络安全水平是相当有益的。例如，EDUCAUSE、通用解决方案组织、Internet2、高等教育信息技术联盟和美国教育联合会等组织可以帮助确定和传授最佳实践方式和通用解决方案。高教部门内负责安全工作的人员还可以参加以信息共享闻名的安全组织，如 CERT、CIAC、SANS、InfraGard 等，它们既是安全的贡献者又是安全的消费者。EDUCAUSE 和界内其他组织可以在共享紧急情况报警方面发挥重要作用。

由于高教部门需要的多种多样，没有哪套最佳实践方式能够适合所有院校。相反，我们的目标应该是提供能够在特定环境下发挥作用多种解决方案。几个事例带来了良好开端。由 EDUCAUSE 和康奈尔大学共同出资创办的计算机政策和法规学院建成了资料来自数百所院校的政策数据库，其政策内容涉及了技术安全的所有方面。

无论使用何种方式，各院校都必须重视以下目标和要求：

- 检测和预防从校园外发起对学校安全系统的攻击。除了盗窃或滥用学校数据等传统威胁外，现在又出现了滥用联网计算机系统的新风险。黑客试图控制校园计算机，将其用作进一步发起攻击的起点或违法走私的仓库。由于这一原因，受害系统的所有者常常看不见已经得逞的攻击。高教部门独一无二地成为这种攻击的目标，由此可见，加强信息共享在高教界显得尤为重要。
- 检测和预防从校内发起针对校外的攻击。即便当黑客利用校内计算机控制了这种攻击的时候，也还是得从学校内部解决问题。拒绝服务攻击的波及面越来越广，制定相应解决方案已经迫在眉睫。
- 确保校园关键系统和数据免受来自校内外的威胁。这个目标也同样适用于美国各个部门的网络空间。这里讨论的信息共享和最佳实践方式可能也同样适用于工业界和政府部门。



## 11. 总结

高等教育部门在美国的网络安全保护工作中发挥着重要作用。它的核心使命教学为国家的未来培养了领导、创新和科技人才。它的科研项目成为很多新知识和由此而问世的新技术的发源地。此外，作为机构实体的大专院校还运行着世界上部分最大规模的计算机群和高速网络。

高教部门正在组织力量研究和解决整个国家都面临的网络安全问题。这是高教界最高领导者的意愿，同时也得到了他们的认可。眼下，各院校已经就传统和创新性解决方案与联邦政府和其他工业部门进行了卓有成效的合作。

总之，高等教育是我国一大重要资源，可用来为网络安全开发解决方案和制定战略规划。它是一个充满科技活力的综合体，需要并且能够接触广泛的信息，同时也需要并且能够实现灵活高速的通信。高等教育的开放性创新价值最终体现为我们国家的开放性创新价值。在很多情况下，高等教育部门的计算机和网络代表着未来的新兴系统。高等教育部门成功的安全保护可以为整个国家树立榜样。

---

## 十三、美国化学部门网络安全战略（摘要）

——调动技术、过程和人员的力量保护化学部门网络安全，降低社会和经济风险

美国化学部门网络安全信息共享论坛  
网络安全战略工作组  
2002 年 7 月

---



扫描二维码阅读全文

## 执行摘要

化学部门为现代生活提供了必需品。由于它触及了生活和商业运作的很多方面，因此，通信技术、相互连接和信息交流是本部门所有公司经营和运转必不可少的条件。然而，使公司经营和运转得以更高效进行的技术也会带来新的脆弱性。正如世界面临着不断增多的威胁一样，化学部门也需要增强能力控制信息安全风险，应对信息被未经授权用于推动或发起物理攻击的威胁。网络安全是整体安全不可分割的一个组成部分，化学工业将在整个部门内采取风险防范措施，以将信息安全风险对公共安全和经济的潜在影响降到最低程度。

降低目前和将来信息安全风险的工作，要求化学部门综合采用尖端技术、业界普遍认可的实践措施和及时的全部门信息共享等措施。幸运的是，当前倡导的为解决网络安全问题全部门通力合作的做法，在化学部门的历史上早已有很多先例。很多已被实践证明行之有效的现成方案可以帮助本部门应对当前的威胁，其中，从应急通信网络到全球性行业协会和标准化组织，为改进当前安全程序和建立未来网络安全实践标准而提供的基础性帮助，堪称不胜枚举。长期主动贯彻国家标准，大力支持研发工作，积极与地方、州和联邦政府机构合作，这种安全文化是化学部门的另一大优势。

由全球性化学部门贸易协会和代表本部门各环节的单个公司最近组成的化学部门网络信息安全共享论坛，制定了一项指导业界相关工作的部门网络安全战略。战略中的建议包括：制定一项“化学部门网络安全计划”，侧重于网络安全风险的控制和消除，提供公开的安全信息和程序控制系统，以帮助保护业界和合作业务的运行。这项基于风险的计划可以满足本部门各个环节和各类公司的普遍和特殊需要。

本计划涉及推动整个部门参与和承担义务、制定一项网络安全公共事务计划、确立自愿性部门实践措施和标准、建立信息共享网络以及推动不断改善的安全技术和解决方案的开发加速进行。本计划呼吁借助共同的知识、共享的技术以及实践措施的开发，建立全行业自愿性实践措施和标准。所提议的网络安全信息共享网络将预先发布有关网络安全威胁、脆弱性和事件的警报。本计划还将推动化学部门与 IT 产品及服务供应商、政府部门和学术界之间的合作，共同开发技术和方法，以高效率解决已确定的脆弱性问题。

在实现网络安全目标的过程中，化学部门应该充分调动技术、程序和人员的力量，通过积极合作处理对整个世界都有严重影响的安全问题。本部门要承担起在国家反恐斗争第一线发挥重要作用的责任，为保护私有财产信息、实现安全运营和保护我们的生活方式而制定标准、开发产品和创造最佳实践措施。

## 1. 化学部门的背景<sup>①</sup>

化学部门是确保国家经济稳定、国土安全以及社会福祉的一大基本要素。作为关键基础设施部门之一的化学工业，为美国经济和生活方式提供必需品已有很长历史。它制造和生产了 70 多万种产品，其中包括基本和中间化学品、专用化学制剂、农用化学制品、化肥、石化产品、

<sup>①</sup> “化学部门的背景”一节的资料来源包括美国化学联合会（ACC）、化学工业数据交流组织（CIDX）和化肥学会（TFI）提供的信息。

塑料和纤维、油漆、涂料和医药品。产值高达 4 500 亿美元的化学部门直接雇用了 100 多万美国人，同时在美国经济中提供了另外 500 万个相关就业机会。美国的食物、安全供水、服装、居所、医疗卫生、计算机技术、交通运输以及现代生活的其他很多方面全都与化学息息相关。

国家研究理事会的一项分析发现，美国经济有 20% 是借助催化作用产生的，而这仅仅是无数化学处理过程中的一种。本部门价值超过 970 亿美元的产品专供医疗保健使用。现代化学支撑着其他经济支柱行业，如农业、通信、建筑和汽车工业等。化学部门是国家最大的出口行业，每年有 800 亿美元商品出口，占美国出口总额的 1/10。化学工业比其他制造业的工资高出 1/3，每年投资 300 亿美元开展研发活动，美国专利商标局每发布 7 项专利，其中就会有 1 项是化学方面的。

化学部门的安全和可靠可使所有其他关键基础设施部门受益，因为这些部门依赖化学产品的安全供应服务于国家安全、国防和社会福祉。含硅化学制品和光纤构成了庞大的美国通信基础设施，从计算机网和互联网到电网和供水网，全国所有城市都被连接到一起。化学产品同时也是我们生活不可或缺的必需品——从推动医疗保健，到提高用于修建住宅和制造汽车的产品安全性和性能，再到提供促使供全世界人民食用的农作物生长的植物营养素，堪称无所不及。化学创新也导致药品创新，从而消除了很多疾病，缩短了医院治疗疾病的时间。

### 安全历史与风险控制

化学部门非常了解自己的价值及其对社会和经济的影响。该部门对风险因素以及控制风险的责任也有十分清醒的认识。成千上万训练有素的化学家、工程师和操作员都是控制和减少与生产化学制品相关风险的专家。

化学部门长期实施各种自愿性方案和计划，大力支持政府标准和研究，长期与地方、州和联邦政府机构有效合作，这些都充分体现了该部门为安全稳定付出的努力。从用于抗击生化战的消毒剂和抗生素，到用于制造钢盔和防弹衣的防火纤维，再到装备安治安部队的智能微处理器，化学部门生产着各种各样的产品，因此可以说，它是军事和公共安全的一支重要力量。

风险是脆弱性、威胁和后果的结合产物。信息与通信基础设施已经成为化学部门运转的关键成分。通信技术和有控制的商务信息共享是所有业内公司经营运转的重要方面。然而，这些使业务工作更快捷、更有效的技术也带来了新的脆弱性。如今，在世界面临威胁日渐增多的情况下，化学部门需要提高控制信息安全风险的能力。它应致力于加强整个行业对风险的认识，从而将影响社会安全 and 经济稳定的后果降至最低程度。

降低信息安全风险的工作要求将先进技术、得到业界普遍认可的实践措施以及整个部门的及时信息共享，融为一体。全部门上下协同合作，共同化解眼前风险，这在化学工业领域已有很多先例。该部门有着快速做出反应、积极解决重要问题的优良传统——从“千年虫”到电子商务事件反应和标准，无不如此。

“9·11”事件重新定义了威胁的范围，然而网络安全问题早在“9·11”事件之前就已经出现在化学部门的雷达屏幕上了。非常幸运，化学部门很早就已起草和论证了相关计划，这为改善当今的安全程序和为未来开发更出色的安全实践措施奠定了坚实的基础。

### 业界政府合作

在了解和把握化学制品与公众健康和环境之间的交互影响方面，化学部门与政府有着相互合作的悠久历史。化学部门通过与国防部、联邦调查局、环境保护局、交通部、联邦应急管理

局、能源部、海岸警卫队以及其他很多机构的紧密合作，把联邦政府的安全保护特长融入了本行业的创新。

### 化学部门网络安全信息共享论坛

化学工业一贯业绩优良，这得益于本行业自觉制定并始终坚持实施严格目标和标准。化学部门在世界范围内构成了一个强有力的合作贸易协会家族。这些组织使本部门得以迅速通过积极合作解决所面临的问题。也正是这种协同合作精神，使化学部门的贸易组织团结了业内 2 000 多家公司，通过化学部门网络安全信息共享论坛投身到解决网络安全问题的工作中来。

为了充分体现整个部门的关注目标和利益，化学部门网络安全信息共享论坛由业界众多贸易协会以及代表本部门各环节的单个公司组成。参与论坛工作的都是公司和贸易协会的高级官员，所代表的贸易协会包括：

- 美国化学联合会；
- 氯元素学会；
- 压缩气体协会；
- 消费者专业产品协会；
- CropLife 美国及农业组织；
- 危险物品顾问理事会；
- 化肥学会；
- 炸药制造商协会；
- 全国化学制品批发商协会；
- 全国油漆和涂料协会；
- 肥皂和清洁剂协会；
- 合成有机化学制品制造商协会。

## 2. 情况分析

网络安全包括信息安全和程序控制安全，是化学部门整体安全不可分割的一个组成部分。我们在对化学部门的网络安全状况进行评估的过程中，必须对网络安全的当前状态和理想状态做出分析，在信息安全和程序控制安全两个方面都是如此。随着程序控制系统越来越强大，与工程设计和维护系统连接得越来越紧密，信息安全对于程序控制也变得更加重要了。过去，信息系统和程序控制系统在一个组织内基本上是分立的。尽管这两种系统的相互结合在恰当的控制下还是安全可靠的，但是整个化学部门整体化、自动化和高度连接的发展趋势已经把本部门暴露在未经授权访问信息的威胁之下，而信息的未经授权访问极有可能被用来从世界任何地方发动物理攻击或制造灾难。

以下对信息系统安全和程序控制系统安全的当前状态和理想状态的评估，以及对安全发展趋势和安全差距的详细分析，为所建议的部门网络安全战略提供了一个基本框架。以下情况分析仅仅是对整个部门特点的一个总体概括，并不全面涉及具体问题。

## 网络安全的当前状况

网络安全在化学部门并不是新课题，已有很多措施被用来确保我们的信息和操作的安全。本部门在程序安全以及标准制定和应用方面有着丰富的经验，这些方面的专业知识将有利于解决网络安全的新问题。

### （1）部门实践措施和标准

化学部门对标准的价值有充分的认识，将其视为统一实践措施、降低复杂性和根据统一基准评估全行业表现的一种有效手段。关于信息安全存在着很多行业标准。然而，在哪些实践措施应在全部门采用、哪些信息应得到保护的问题上，业内人士还没有取得一致意见或形成统一认识。由于程序安全是设计方案时必须考虑的首要 and 重要因素，因此业内很多公司都在程序中采用了惯常的实践措施。部门参与者在自动化、安全实践措施和技术水平等方面的参差不齐，把脆弱性带入了供应链。参与者面临的风险因所制造或销售的产品、相关的危险以及潜在的信息安全风险的不同而各异。目前，已有越来越多的外部供应商和承包商能够进入本部门网络和接触相关敏感信息，信息系统的范围已经扩大到具有全球化的性质。所有这些因素都增加了我们面对网络恐怖主义攻击的脆弱性。

### （2）技术和程序

从原料采购到产品制造，从后勤保障到产品销售，从客户服务到财务审计，信息技术在化学部门的企业运作中发挥着关键性作用，不论公司规模大小，概莫能外。当前，本部门采用现有的高科技工具保护网络系统的安全运行，但是，大部分保护措施都是针对互联网的。风险显然绝不仅仅限于互联网。而且，安全也绝不仅仅依靠买回一种工具就能实现，它还要依赖组织内的管理政策、操作规程和用户的行为，同时也要依赖单个公司对事件的反应能力。

随着公司内部以及公司之间相互连接得越来越紧密，化学部门计算机系统生命周期的延长、越来越多新旧系统的相互衔接以及部门内使用非定制技术的增多，在系统差异和接口处产生了很多潜在脆弱性。另外，目前虽然已有很多软件业的实践措施被应用到商业化用途、基础设施和安全计划之中，但它们没有接受过严格的网络安全脆弱性验证，因此极有可能含有新的网络安全脆弱性。

有些在公司办公和程序控制中使用的现行实践措施需要得到重新审视，其中包括口令保护屏保和缺乏通过用户名和口令限制物理进入计算机的手段。当前，这些问题都是在公司层面上解决的。尽管有些大公司通过采用新的网络结构设计和加强访问控制而减少了面对网络攻击的脆弱性，但是确保安全仍然是设备使用者应该承担的责任，而且个人用户依旧有可能对安全实践措施的效果产生负面影响。

迄今为止，化学部门还没有一项信息共享方案是针对网络安全破坏行为提出的。对潜在民事和刑事责任风险的担心，以及对暴露给政府的信息会被不适宜第三方访问的担心，会成为建立信息共享机制的障碍。

### （3）验证

在化学行业内，验证政策和标准执行情况的工作通常是内部和外部审计部门的共同责任。尽管有些业内组织在服务供应商和其他第三方进入内部环境之前采取了对其进行验证评估的做法，但是这种审计并没有在整个部门普遍实施。化学部门内目前还没有统一的审计标准，不过，已有很多部门性标准化组织和行业机构开始着手解决与网络安全相关的某些问题。

## 网络安全的发展趋势

业内公司依赖信息技术保持自己的竞争力。由于自动化程度越来越高、外部威胁愈演愈烈，本部门始终在不断利用新技术和改进中的实践措施解决安全问题。商业和技术的发展趋势推动了经营、技术和商业实践的不断变化，导致信息技术的利用和集成达到一个新的高度，从而减少了脆弱性和风险。会对信息系统和程序控制系统的安全产生影响的发展趋势包括业务程序的重新设计、竞争压力、电子商务与供应链的融合程度越来越高、外购的不断增加、企业结盟和合资企业、商品技术利用程度不断提高、技术的快速发展以及多工作点和全球性操作的连接。

## 理想的网络安全状况

确保化学部门网络安全的目的是保护信息的保密性、完整性和可利用性以及控制程序的安全性和有效性，同时也是为了预防信息被用来破坏本部门公司的物理安全。要想有效实现这些控制目标，不仅需要技术，同时还需要程序和人员。

理想状况是，网络安全得到公司管理层的大力支持，网络安全被视为与其他方面的安全同等重要。有了这样的支持，很多网络安全问题便可以在本部门的公司内部得到解决。标准化语言和方法被用来确保公司之间电子交往的安全。企业内信息安全、物理安全、保健和环保、采购和销售等不同部门表现出高度的协调一致。

## 网络安全差距

本行业的当前状况与理想状态之间的差异就是必须弥补的具体差距。其中很多差距可以在本部门内解决，但是其余差距则需通过与其他使用程序控制系统的行业之间的合作加以解决，其中包括造纸、食品加工、电力、石油和天然气以及其他加工行业。

### （1）自愿性部门实践措施和标准

尽管化学部门显示出对关键性问题进行严格管理、有效合作和快速反应的能力，但是部门内在涉及网络安全的自愿性标准和通用实践措施方面还没有实现统一。本部门需要开发适用于整个部门的安全实践措施，其中包括（但不限于）涉及用户资格有效电子确认的自愿性标准实践措施、基准工具和通用风险管理方法等。

### （2）技术和程序

供应商当前提供的产品需要在安全方面有所改进。然而，技术供应商是不会单独为化学部门主动升级产品的安全性能的。因此，整个化学部门的各个分支之间需要通过合作来缩小和弥补当前存在的技术差距，从而在以下关键方面提高安全水平：开放系统、软件质量、身份鉴别、远程登录、网络管理、无线通信、企业系统和访问程序控制系统。

### （3）验证

由于化学部门内有越来越多的公司通过网络相互连接，因此就更需要确保所有部门贸易伙伴（其中包括延伸的产品供应链伙伴）遵守已公认的自愿性网络安全实践措施和标准。目前，化学部门缺乏有关网络安全的认证程序和服务，同时还缺乏用以确定供应链伙伴资格的自我评估工具和高效率方法。

### 3. 美国化学部门网络安全战略建议

全球性的化学部门有着积极应对安全问题的悠久历史。以往，化学部门的领导者和各方专家共同分析问题、制定最佳战略、调动人员积极性，从而使社会、环境 and 经济大受裨益，这充分显示了该部门统一全行业认识、上下同心协力应对挑战的能力。对于眼下的网络安全问题，化学部门也将采取协同合作的相同方式应对。

本战略旨在通过增强化学部门的网络安全来帮助保护人员、财产、产品、程序、资料和信息。虽然本战略的侧重点在美国国内，但是由于化学部门是一个全球性行业，因此任何建议都必须考虑本部门的全球化性质。

所建议的计划（以下简称“本计划”）基于一系列整体化要素，旨在把网络安全的问题提高到关系业内公司安全的高度，鼓励企业决策者带头制定或加强安全政策和计划。化学部门应在适用法律允许的范围内协同合作，加强信息和程序控制安全的设计和管理，以不断改善整个部门的网络安全表现。所制定的自愿性实践措施和标准应该与风险、威胁和脆弱性的程度相适应。

#### 指导原则

为了完全满足业内各环节大小公司的网络安全需要，化学部门应遵循以下原则制定网络安全计划。

- 认识到网络安全是整体安全不可分割的一个组成部分，应以遵循“履行责任全法典”等化学部门安全方案的原则和实践措施开展工作。
- 认识到化学部门是与其他关键基础设施部门乃至全球经济高度结合为一个整体的。
- 认识到有效的网络风险管理要从董事会和行政管理的高层做起。
- 开发基于原则和程序并适用于化学部门内多种成员以及各种风险和后果情况的解决方案。
- 同时考虑企业内具体网络安全脆弱性和企业间网络安全脆弱性。
- 强调全球性化学部门需要的做法应该与美国的国家需要保持一致。
- 调动和加强本部门内的网络安全专业力量，同时吸收其他部门的专业人员。
- 确保化学部门网络安全战略和计划跟上变化的步伐。
- 鼓励所有有资格的化学部门供应链参与者（其中包括消费者、运输者、供应商、批发商、技术和服务供应商、承包商等）全部参与到保护网络安全的工作中来。

#### 战略意图

本行业将执行一项“化学部门网络安全计划”，侧重于管理和减少网络安全风险，以提供开放但安全的信息和程序控制系统，从而帮助保护整个行业的安全和促进全行业的密切合作。这项网络安全全面计划将提供一种改善化学部门信息及信息基础实施安全状况的手段，同时合理分配资源以有效确立以下关键性计划要素：

- 推动参与并确定责任；
- 制定一项网络安全公共事务方案；
- 制定自愿性部门实践措施和标准；
- 建立一个信息共享网络；



- 鼓励加速开发不断改进的安全技术和解决方案。

### 推动参与并确定责任

全部门各环节均广泛支持和积极参与是本项提议计划成功的关键。一个“领导论坛”行将建立并向所有有资格的本部门参与者开放，以推动整个部门参与网络安全工作并承担相应责任。本计划的总体实施和长期运转是领导论坛的责任，它将为计划的发展提供和安排资金，促使本战略阐述的化学部门网络安全方案的各个关键要素得到落实。

领导论坛的目标是：

- 通过在整个部门内以及对社会公众、利益相关人和雇员实施教育和信息交流计划，大幅度提高人们对网络安全问题的认识 and 了解。
- 详细说明潜在网络破坏事件对商业、经济和社会的潜在影响、后果和意义。
- 推动管理层关注和领导有关网络安全问题的的工作。
- 确定“化学部门网络安全计划”的职责。
- 争取各贸易协会和标准化组织以采纳、认可和执行等行动给予支持。
- 制定一项网络安全公共事务方案。

领导论坛将借助贸易协会、标准化组织和专业组织的现有网络建立和实施本计划必要的各个要素。

为了推动自愿性部门实践措施和标准的开发和鼓励加速改进技术和解决方案，一个“利益社区”行将建立，目的是在本部门专业人员之间以及与其他部门的专家、技术供应商和其他供应链伙伴交流专业知识、技术和实践措施。本计划将寻求现有信息技术和程序控制标准化组织和专业组织的参与和支持。

同样，领导论坛也将与现有组织和部门专家密切合作，共同开发和建立一个信息共享网络，同时对网络安全公共事务方案实施领导。

在建立这一资源网络和利益社区的过程中，领导论坛还将主持提高认识、开展教育和培训等活动，以提高对这些问题以及对在化学部门内积极加强网络安全的潜在意义和重要性的认识。活动可能包括部门参与者、供应链伙伴、承包商、服务和技术供应商的培训和指导并安排实习，以提高他们的认识和增强他们的能力。

现有的化学部门网络安全信息共享论坛可能会经转变后成为领导论坛。

### 建立网络安全公共事务项目

开放的信息共享是充分发挥化学部门网络安全项目作用所必不可少的。领导论坛将为有资格的部门参与者提供密切合作的机会，使他们得以共同制定出部门实践措施和政策，推动信息共享，以达到减少网络安全风险的目的。

寻求政府协助可鼓励制定相关公共政策和规定，用以在部门内就如何降低网络安全风险、争取网络安全投资纳税优惠等问题开展必要和适宜的交流和信息共享。需要解决的潜在问题可能包括：

- 免受可能禁止或阻碍业界合作的任何限制性反托拉斯法的制约；
- 减少承担额外责任；
- 某些类型共享信息豁免《信息自由法》；
- 处理好网络安全与隐私权之间的矛盾关系；

- 通过经济刺激推动网络安全技术的开发和投资。

### 制定自愿性部门实践措施和标准

有资格的化学部门参与者应该投身于制定适于整个部门的自愿性管理实践措施、程序、方针和标准的工作之中，以支持整个部门实现预期目标和履行自己应尽的公司管理责任。

虽然化学部门各环节的业务和信息系统所面临的风险差异很大，甚至同一环节内不同类型的公司之间也存在差别，但很多通用原则、程序和实践措施可被所有公司用来为每种具体情况标识和确定保护网络安全的适宜手段。自愿性部门实践措施和标准是保护信息保密性、完整性和可用性的必要条件。这些实践措施和标准要想成功，就必须公开、中性和免费取用。

领导论坛将根据相关法律规定确定自己的工作任务。

- 建立一个利益社区，把网络安全专家和其他学科专家组织到一起，对部门实践措施的实施提供指导和专业支持。
- 从本部门收集现行实践措施并进行评估，同时借助其他部门、标准化组织和专业组织的知识和技术，最终达到减少化学部门脆弱性的目的。
- 创建、运行和维护有关潜在脆弱性和可能的已知解决方案的资料库。
- 推荐（必要时开发）化学部门所需的自愿性部门实践措施和标准。
- 建立一套用以评估安全表现等级的程序，同时为审计和验证工作设置适宜程序并提供支持。
- 作为“业界喉舌”要求技术供应商和研究人员开发可以满足化学部门需要的解决方案。

#### (1) 利益社区

网络安全利益社区将共同对化学部门各环节共同和特殊的网络安全脆弱性、威胁和风险进行评估。评估任务将在领导论坛建立的指定标准化组织的帮助下实施。

利益社区将为业内公司提供一个交流网络安全知识和经验的论坛。业内公司将有机会与本部门专业人员以及来自技术供应商、供应链参与者和相关部门的专家共同探讨网络安全问题。这些问题包括：

- 确定和分析化学部门的潜在网络安全脆弱性、风险和后果。
- 确定、分析和建议应该着重关注并应努力减轻其后果的风险。
- 就可用的解决方案建立和维护一个数据库，供业内公司及其供应链伙伴参考使用。

该组织将在选择和 / 或开发自愿性实践措施、指导方针和适用标准方面，以及在推广和支持用以满足本部门需要的适宜风险评估方法和管理手段方面，在部门内广泛寻求支持和参与。

#### (2) 开发自愿性部门实践措施、指导方针和适用标准

指定的标准化组织将引导用于与本计划结合的部门实践措施、指导方针以及适宜的支持性材料和服务的开发和采用。该组织可能还会在适当的时候建议在全部门采用基于风险的自愿性安全和可靠性标准。

所建议的自愿性部门实践措施和标准应是基于风险并针对本部门各环节以及有资格的参与者的常见问题的。所建议的任何方法和系统都应在购买力之内并且是能够升级的，因此，解决方案能够被所有公司有效实施。有关支持方案实施的服务和方式选择的情况介绍应经整理后汇集成册出版一本参考指南。

要到适宜的标准化组织建立并运行之后，有关哪些具体方面的问题需要解决的确定和选择

工作方可开始进行。在本战略支持的初步工作的基础上，需要探索的方面可能包括：

- 制定确保公司网络安全可靠的计划的方法。
- 用于评估网络安全风险的方法（可以作为总体安全风险评估方法的一个组成部分）。
- 针对具体网络安全活动的部门实践措施，其中包括（但不限于）身份管理实践措施、信息分类方法、远程登录、贸易伙伴资格、验证程序和工具以及表现评定和计分卡等。
- 所建议的针对具体网络安全技术的表现评定等级，其中包括（但不限于）密码编制、病毒检测水平、实时监控和入侵检测。

作为开发程序的一部分，标准化组织将对各种现有选择做出评估，侧重于针对本部门确实特有的问题开发解决方案。化学部门将寻求借助得自其他标准化活动的现有实践措施、指南、材料和服务来满足本部门的需要。此外，本部门还将参与和 / 或领导跨部门方案的制定工作，以满足化学部门的需要。

### （3）建议的公司网络安全计划

与总体安全实践措施相一致，标准化组织所要考虑的首要问题之一是，为制定一项适用于所有有资格的本行业参与者的“公司网络安全计划”开发建议性原则、方法和支持性材料。尽管每个公司的系统、操作、脆弱性和风险各异，但是所有公司都可以通过一个通用框架和程序制定出适合于整个部门的计划。

来自本部门各个环节的专业人员应密切合作，共同开发和建议实施一项可以满足本部门各环节和各类公司共同和特殊需要的针对网络风险的计划。这个计划应是总体安全计划的组成部分，它的重要元素可能包括以下几个。

- 管理层的支持：网络安全应被视为公司结构体系的一个重点问题，对这个问题的认识和重视是一个不断努力的过程，同时，计划的运行还应在资金上得到适当考虑。
- 制定内部政策和自愿性标准：公司应刻意将所制定的政策和程序形成书面文件，以显示管理层对网络安全预期的支持并准备承担责任。相关政策和自愿性标准应是针对风险及其潜在后果的。
- 风险评估和管理：对网络安全风险的确认和分析应成为一项日常工作，而通过经验证有效的风险评估方法减少风险的工作也应持续进行。网络安全风险评估应与物理安全评估协调进行。信息分类则是风险管理程序的另一个重要组成部分。
- 身份管理：公司应该使用可以应对信息暴露风险的鉴别技术。公司还应对有权进入关键资源的用户进行筛选甄别（即调查用户的背景）。
- 安全监控和措施：化学部门的公司应该开发和维持安全措施的有效性，其中包括基于技术的控制和管理控制。
- 安全意识：化学部门应为提高业内人员的网络安全意识制定总体指导原则。所有公司都应对授权使用和维护信息资源的人员进行适宜程度的教育和培训，以提高他们的安全意识。
- 安全与隐私：化学部门的公司必须以恰当措施保护公司及员工的敏感信息。此外，还应建立数据分类的指导机制。
- 数据储存和传送：对外公开的数据和通过公共网络传送的数据都应受到与信息安全风险相应的安全级别的保护。化学部门应制定确定和保护处于风险下的信息的指导原则。

- 应用软件：无论是开发的还是购买的信息系统，对它们的哪怕是最低的安全功能要求，也应规定到与风险级别相应的指导原则中。
- 网络配置管理：公司在将其内部网络与互联网或其他公司的网络连接时，应格外小心。公司在建立内部网络时，应采用适当的技术来保护实体的信息资产，同时减少由连接带来的责任问题。
- 变化管理：网络结构和应用系统应该跟随用来保护生产环境的稳定性和完整性的变化管理程序的变化而变化。
- 事件反应和运作的持续性：公司应制定一项经过检验并正式成文的事件反应计划，用以说明如果出现可疑或真实入侵事件应该采取什么行动。这项计划应包括事件发生前后的处理程序以及保持企业运作持续进行的措施。
- 审计：公司应要求对安全计划和程序以及自我评估进行内部和外部审核，以确定程序得到遵守和找出可能由新情况造成的安全差距。

#### （4）可能的组成和结构

致力于电子商务标准研究的化学工业数据交流组织（CIDX）可能会被指定为负责化学部门自愿性网络安全实践措施和标准的标准化组织。去年，CIDX 在全球范围内成功推广了化学工业电子商务标准（Cheme Standards），这项基于 XML 的标准是专门为化学公司及其贸易伙伴之间的电子商务交易而制定的。目前，欧美已有约 50% 的国内化学品交易是通过电子商务的方式完成的。

CIDX 是根据《美国法典》第 501（c）3 节建立的一个公司式组织，成立于 1985 年，在法律、政策和管理结构完备的条件下得到了充分发展。成员对象是化学部门所有有资格的公司，其中包括化学产品各生产环节的公司、供应链伙伴、服务和技术供应商。

#### 建立信息共享网络

化学部门将正式建立一个网络安全信息共享网络（以下简称“网络”），用以就网络安全威胁、脆弱性和事件发出预警。建立该预警系统的目的是为了标识和减少基础设施的脆弱性、抗击网络攻击或从破坏中迅速恢复。

最初，信息共享网络将侧重于以下方面：

- 在紧急情况下提供可供选择的安全通信。
- 高成本效益传播收集自监控服务、政府部门和其他资源的有关信息和物理系统受到威胁的信息。
- 就具体事件的决议和解决方案提供进入第三方数据库的方便。

至于与专属信息相关的公共事务问题，本部门将探究扩大信息共享网络的范围，从而为与事件、威胁和脆弱性相关的信息以及决议和解决方案的匿名和保密共享提供一种安全可靠的工具。信息共享网络的扩展功能中还将包括就得自其他部门的信息向政府部门提供有综合分析内容的报告信息，同时还将把得自政府部门的分析结果和预警传播给化学部门。

最终，该“网络”的主要目标如下：

- 提供一种安全可靠的工具，使有关事件、威胁、脆弱性、决议和解决方案的信息输入和共享得以在经过鉴别和匿名的条件下顺利进行。
- 允许成员就其身边的事件、威胁、脆弱性、决议和解决方案自愿提供信息。这样，提

交的信息可以使“该系统”判断信息是否与会波及整个部门的规模更大的事件相关。

- 提前公布有关于对化学部门及其相关行业的信息系统和物理系统造成威胁的通报和警报。
- 就化学部门内以及供应链相关环节内的信息和物理系统所受到的威胁发出预警和早期警报。
- 就具体事件提供决议和解决方案建立数据库，数据库将向该“网络”所有成员开放。
- 就事件及其对整个部门的影响向该系统成员提供分析信息。

#### （1）可能的组成和结构

CHEMTREC 是美国化学联合会属下的 HAZMAT 事件反应处理中心，它对提议中的信息共享网络的建立和运转可能具有潜在帮助。该“网络”可以签署服务合同的方式由美国化学联合会运营，化学部门有资格的参与者均可加入。

该“网络”的设施应确保物理安全，系统的各个成分都应通过先进安全技术加以保护，其中包括对未经授权进入、改动或破坏系统企图的实时监控。

#### （2）加入

由于化学部门与其他行业已经广泛融合为一体，同时由于整个供应链所面临的网络安全风险的系统化性质，该“网络”的服务应该指明特定部分供所有有资格的供应链参与者和政府部门代表加入。然而，出于为共享的敏感和财产信息保密和避免因共享敏感信息而产生新的威胁或脆弱性的目的，该“网络”服务的某些部分仅限于化学部门公司的指定和有资格的代表享用。

#### （3）信息来源

该“网络”将与全球范围内的信息来源和服务合作，就信息硬件和软件产品、程序控制系统、物理安全等方面的内容最广泛地提供有关威胁、脆弱性和事件的数据。信息来源包括以下方面。

- 成员公司：成员公司的网络安全专业人员将能自愿报告有关完全威胁、脆弱性、事件和解决方案的信息（匿名和署名方式均可）。
- 行业专家组织和论坛将对业界特定需要做出评估并制定自愿性部门实践措施和标准（通过指定的标准化组织）。
- 技术供应商（如微软、IBM 和 AspenTech 公司）。
- 安全协会（如 CERT 和 SANS）。
- 互联网资源（如公告版和新闻组）。
- 其他行业的信息共享网络。
- 州、联邦和外国政府部门和执法机构（如 InfraGard）。

上述来源的信息将接受可用性和潜在解决方案确定方面的评估。该“网络”将根据得到一致认可的严重程度分类向成员发出预警通报。

#### 鼓励安全技术的改进和解决方案的开发加速进行

部门参与者将与 IT 产品和服务供应商、政府机构和学术界积极合作，加快不断改进的技术和方法的开发和投入使用，以高效解决得到确定的脆弱性问题。各方面的课题专家将依照结构严密的程序领导这些活动。

化学部门将在利益社区领导下与产品供应商密切合作，就产品开发的方向提出意见。这种

与技术伙伴的合作关系有助于本部门影响技术的变化，从而更好地满足安全、稳定和整体化企业运作的需要。

这种合作方案还将寻求与其他行业需求相同的伙伴以及与政府和学术界的合作，以推动技术研发工作加速展开，不断提高网络安全水平。

需要考虑的问题可能包括：

- 用以评估潜在威胁和脆弱性可能给化学部门造成的后果的模型；
- 对程序控制系统的入侵的实时检测；
- 情报、安全风险和脆弱性评估；
- 在安全与高成本效益商品技术之间找到最佳平衡点；
- 供应商和第三方评估；
- 风险评估方法；
- 适用于不同操作平台的标准化安全软件。

#### 计划总结

化学部门将在适用法律允许的范围内与供应链伙伴展开合作，推动用于保护关键信息、信息系统和程序控制系统的自愿性部门标准、产品和实践措施的开发和制定工作。化学部门的公司将充分调动技术、程序和人员的力量，通过各种实践措施，保护财产信息资源免受未经授权进入或破坏，加强部门设施的安全稳定运行。这要求选定的标准制定组织加强工作，同时要求本部门公司与 IT 供应商密切合作，提供产品开发方向的信息。

---

## 十四、电力部门对关键基础设施保护挑战 的回应（摘要）

北美电力可靠性委员会

2002 年 5 月

---



扫二维码阅读全文

## 1. 介绍

我们的经济、技术和国家安全环境正在发生着巨大变化，北美电力基础设施就是在这样的环境中生存和运转的。基础设施（尤其是电子系统）的持续而可靠的完整性遇到了前所未有的新威胁，所表现出来的脆弱性正在迅速形成。电力部门有着同心协力确保北美电力系统可靠性的悠久历史，因此会认真对待影响这种可靠性中的任何新问题。电力部门可能会灵活采用的一种行动方案<sup>①</sup>是：

- （1）认识到本行业在哪些方面因合作结构、政策和流程的完备而做得十分出色。
- （2）确定我们的环境中有哪些方面由于我们将关键基础设施保护 / 资产风险管理成功经验应用到新出现的物理和电子威胁上而出现了变化。
- （3）将现有流程和结构用于解决新问题（运用北美电力可靠性委员会(NERC)、地区委员会和单个组织的现成模式）。
- （4）加强电力部门内各方合作以提高行动效率（通过合作组织、电力可靠性委员会和各贸易协会加强业内合作）。
- （5）与涉及本行业的政府机构以及其他经济部门合作，共同确定和解决角色、互依赖性和障碍问题（对政府角色、研发、法律和政策等问题给出明确界定）。

## 2. 方案概述

确保国家电力基础设施正常传输电力是我们行业每天的基本工作。由于电是社会核心活动的基础，消费者和公众的预期会形成一种压力，促使业界成员为保护和管理对于电力系统可靠性和完整性来说至关重要的物理和电子资产而付出辛勤努力。

北美的电力系统高度互联，多年来，整个行业在应对自然灾害、恶意行为和其他危机的过程中形成了三级服务保障机制。

- 北美电力可靠性委员会负责就电力供应可靠性问题进行全国性协调以及与加拿大和墨西哥两国进行国际性协调，同时，单个供电机构以及地区委员会与州和地方政府展开合作。
- 各地区与供电机构之间相互连接和相互依赖的本行业历史促进了供电机构与各地区在危机和突发事件时期的密切合作。因此，供电机构不仅重视如何确保自己提供服务的能力，同时还重视自己邻居提供的支持或提出的支持请求。本行业表现出来的突发事件应急能力显示了多重援助计划以及这种互惠合作的价值。
- 其他基础设施与电力部门之间的相互依赖关系非常复杂，需要不断进行分析和评估。

---

① 本文所述“行动方案”是北美电力可靠性委员会关键基础设施保护顾问组 40 名成员精心努力的成果。该顾问组致力于就北美电力系统所受到的威胁和所具有的脆弱性对整个电力部门提供指导性帮助。相关活动涉及物理和电子保护，其中包括监控、检测、培训和演习。顾问组成员包括来自北美电力可靠性委员会地区供电机构成员、电力营销商、独立电力生产商、美国公共电力协会、加拿大电力协会、爱迪生电力学会、电力供应协会、全国乡村电力合作协会、电力研究会、能源部、联邦调查局、国家基础设施保护中心、关键基础设施保障局和北美电力可靠性委员会的代表。顾问组的成就体现了电力部门对待关键基础设施保护工作的认真态度。



多年来，各供电机构与地方电信部门、石油和天然气供应商、其他基础设施以及地方和州政府应急服务机构发展了良好的关系。这种地方关系的重要性已在“千年虫”防范工作中得到认识乃至巩固。此外，联邦政府和一些州正在确定互依赖性并为本行业制定州和地区性应急反应计划进行协调。

本文描述了一个总体行动方案，其内容收入在业界成员、NERC 及其地区委员会用以确保服务的规划和计划中。所实施的具体计划和行动选择依每个组织对自身所受具体威胁、脆弱性、潜在后果、当地社区和消费者的期望以及风险容忍度的评估而定。进行这些考虑时，可用信息越丰富，各个组织乃至整个行业做出的决策就越全面，尤其在新的威胁和脆弱性不断涌现并且被明确确定的情况下。

本行动方案是根据一种常用安全模式制定的，它包括以下内容：

- 确定关键服务以及支持这些服务的资产；
- 评估脆弱性，其中包括分析政策、程序和标准；
- 进行风险评估，其中包括分析缓解措施；
- 制定和检验复原和恢复计划；
- 监控和定期更新评估；
- 共享信息、教育和提高认识；
- 协调电力部门内的活动；
- 了解各关键部门之间的互依赖性；
- 确定并支持研发工作；
- 认识法律法规问题以及实施关键基础设施保护计划遇到的其他挑战。

#### 电力部门关键基础设施保护需要面对哪些具体挑战？

- 认识：加强对不断出现的威胁和脆弱性的了解和重视，外加精确定义物理和信息安全，将其作为电力行业“可靠性”定义的一个基本组成部分。
- 技术：加强对日趋复杂的电子设备的管理，了解技术风险并将其结合到范围更广的企业风险管理程序之中。
- 共享：加强各机构（如 IT、运行和安全机构）内、电力部门参与者之间以及相互依赖的经济部门之间的现有信息交流机制，同时作为联系人加强与政府机构的信息交流。
- 方法：扩大和强化现有的结构体系、政策和程序，用以应对不断出现的物理和电子威胁。
- 改组：确保关键基础设施保护工作不会阻碍行业的改组进程，同时确保行业改组支持关键基础设施保护方案。
- 路线图：为制定和实施安全保护方案制定适宜战略、计划和程序。

### 3. 本行业的历史使命

过去 10 年里，北美电力可靠性委员会（NERC）被数次要求就与国家安全相关的问题担任电力部门主要联系机构。自 20 世纪 80 年代初以来，NERC 先后参与了电磁脉冲现象、州属电

力系统的脆弱性、多点破坏和恐怖活动、“千年虫”影响以及当前迅猛发展的电子入侵和物理攻击等工作。NERC 的使命核心始终是与联邦政府各机构通力合作，共同减少高度互联的电力系统面对这些威胁所表现出来的脆弱性。

关键基础设施保护总统委员会（PCCIP）1997 年 10 月提交的报告导致第 63 号总统令（PDD63）于 1998 年 5 月颁布。该总统令要求各政府机构积极参与“关键基础设施保障国家战略”的制定工作并寻求私营工业参与，以通过公共-私营部门的合作实现保护国家关键基础设施的共同目标。PCCIP 特别称赞 NERC 是私营部门与政府之间信息共享、合作和协调的样板。1998 年 9 月，能源部长致函 NERC 主席，请求 NERC 代表电力部门协助制定一项保护北美大陆电力部门基础设施的方案。NERC 回应美国能源部的要求，同意作为电力部门协调员参与关键基础设施保护方案的制定工作。本文重点说明了 NERC 的美国、加拿大和墨西哥电力部门成员在关键基础设施保护（CIP）/ 资产风险管理活动中可能采取哪些行动。

#### 第 63 号总统令颁布后电力部门完成了哪些工作？

- 建立了一个关键基础设施保护顾问组，其成员广泛代表了北美供电机构成员、其他民生工业组织以及政府部门。顾问组对 NERC 理事会提交多种报告，同时还收集了来自其他行业相关安全委员会（如 EEI、CEA、APPA 和 NRECA）的信息。
- 加强了与联邦政府机构，尤其与联邦调查局、NIPC、教育部、国家实验室、CIAO、乡村公用事业局和加拿大相应机构的合作。
- 发展了与民生工业组织，尤其是与 NERC、EEI、AGA、APPA、NRECA 和 EPRI 之间的合作关系。
- 建立了一个电力部门信息共享和分析中心，用以收集突发事件信息、中转发布预警通报、与联邦调查局/NIPC 以及全国电网运营者共同发布每日简报；制定了提示、分析和预警计划，用以对供电机构相关人员就突发事件报告和预警通报程序进行培训。
- 建立了一个供电机构首席执行官安全委员会，用以加强规划、提高认识和配置资源方面的工作。
- 开展了大量针对行政管理层、安全人员、运营负责人、政府代表和设备供应商的研讨活动，涉及安全意识、脆弱性评估、经验教训以及数字程序控制等多方面的主题。
- 编制了多种安全参考文件，其中包括“（安全）行动方案”、“安全指南”、“（物理和网络事件）威胁预警级别和反应指南”等。
- 制定了相关安全计划，如针对业界成员、政策和程序制定负责人、程序实施负责人、供电线路及电厂安全负责人和风险管理负责人的“EPRI 企业基础设施安全计划”。本行业还应邀派员在各种论坛上演讲，就新出现的安全问题、新决策工具和技术对业界成员进行宣传教育。
- 就各种内部运行和电网运行进行了大量威胁和脆弱性评估工作，在总结以往教训的基础上鼓励各供电机构与其他业界同行交流经验。
- 与其他部门的相关机构，尤其是 PCIS 和其他行业的信息共享和分析中心建立了协作关系。
- 建立了若干个工作组，分别负责信息共、密码编制和关键成分统计等涉及整个部门的工作。

## 4. 电力部门行动方案的要素

本“行动方案”从以下四个层面就如何采取行动应对物理和电子威胁展开论述：避免（如通过政策、程序和提高安全意识计划等）、保障（如定期反复评估风险）、检测（如监控、报告和分析问题）和恢复（调查、修复和交流教训）。本“行动方案”的主要元素可分为以下几个类别。

### 确定关键服务和资产

风险管理的目的是以适当的成本减轻潜在损失带来的潜在后果。关键服务和资产级别可根据任务的关键性以及公众与客户的预期和需要确定。优先重点通常是出于确保公众安全和维护公众信心的目的而确定的。供电机构通常与用户、州和地方政府以及联邦政府共同确定哪些服务和资产级别属于关键的范畴。关键服务和资产级别一旦确定，支持它们的资产应随之得到确定，而管理已知风险的计划也会迅速到位。

评估安全风险的第一步是明确阐述维持任务以及运行和服务正常进行的关键功能，随后是确定支持关键功能的关键资产。这种评估可以揭示这些资产为什么至关重要的原因（也就是哪些属性使它们显得至关重要）以及它们的相对关键程度（也就是定义资产损失或损坏后果的尺度）。物理和电子资产都应被考虑，其中应包括信息基础设施、硬件、软件、数据和信息、人员、文件及供应品。评估既要考虑资产的美元价值，同时也要考虑资产相对于它所支持的任务的价值。

在与客户以及代表公众利益的机构合作时，考虑以下问题可能会有助于决定把哪些电力供应系统基础设施纳入关键资产清单：

- 国家安全：电力基础设施资产的损失或损坏是否会破坏或威胁美国、加拿大或墨西哥军队或政府执行保护国家军事或国民安全任务的能力？
- 公众健康和安全：电力基础设施资产的损失或损坏是否会破坏或威胁公众安全及健康和/或美国、加拿大或墨西哥的环境？
- 经济稳定：电力基础设施资产的损失或损坏是否会破坏或威胁美国、加拿大或墨西哥的经济稳定？
- 地区、国家和北美电网的可靠性：电力基础设施资产的损失或损坏是否会破坏或威胁地区、国家或北美电网的可靠性？
- 发电、输电和配电：电力基础设施资产的损失或损坏是否会破坏或威胁充分满足地区、国家和北美用电需求的电力供应和输送？
- 关键控制系统：电力基础设施资产的损失或损坏是否会破坏或威胁对发电、输电或配电的实时控制？
- 基本业务系统：电力基础设施资产的损失或损坏是否会破坏或威胁对企业运转或政府运作具有巨大影响的运行可靠性和业务系统？

### 脆弱性评估

对物理和电子脆弱性进行评估可以带来以下几点益处：

- 确定会增加风险的实践方法和情况。
- 找到可以降低风险的行动和实践方法。

- 区分后果管理工作中哪些属于战略性的，哪些属于战术性的。
- 将能够对整个企业产生影响的各业务单位的决策结合为一个整体。
- 从资产关键性和所受威胁的角度提供确定重点和配置资源的基本原则。
- 提供确定认识和培训问题的基础。

评估安全风险的工作包括通过查阅书面记录（如制定了哪些规章/规定）、接触人员（如人员发挥了什么作用/对安全的感受如何）、走访现场（如系统是如何安装和运转的）以及进行测试（如系统和人员怎样应对攻击）等方式评估脆弱性。

采纳本“行动方案”时，应在物理和电子脆弱性评估中考虑以下因素：

- 网络结构：网络布局、主要信息资产、加密通信协议、登录控制、入侵检测和预警报告。
- 渗透性测试：模拟外部威胁、内部威胁和社会工程、战争拨号等具体入侵的测试。
- 物理安全：登录控制、入侵检测设备、相关预警报告和显示、通信设备、灯光、电源和保护力量。
- 物理资产分析：资产利用、系统冗余和与其他基础设施的相互依赖。
- 运行安全：拒绝敌人登录那些可能会不恰当帮助任何个人或组织对市场或系统运转造成不良影响的敏感或非敏感信息。
- 政策和流程：检查业务程序，以便①确定影响安全的关键因素；②使遵守、实施和执行得以有效进行；③参照或遵守已制定的标准；④提供明确的全面指导；⑤有效确定角色、责任、职权和义务。

### 风险评估和风险管理

关键基础设施保障一直被业界视为一种风险管理过程。然而，在当今的环境中评估和管理安全风险，意味着要以一种全新的视角看待包含在企业全面风险评估中的问题。除了要认识与企业运营相关的常见风险因素外，在更广的视角下可能还包括以下问题：

- 金融风险；
- 环境风险；
- 安全风险；
- 供应风险（如燃料、水、备件等）；
- 建筑和承包商风险；
- 保险风险；
- 国内国际政治和法规风险；
- 品牌资产风险；
- 稳定风险。

一项风险管理计划通常要包括对各种行动的不同级别的投资，其中从预防和阻止，到管理和减少意外事件，再到反应和恢复，行动范围极广。对如此之多的行动如何做出投资取舍，往往取决于对威胁或脆弱性、投资可行性以及后果可预测性的了解。例如，有些服务于极易遭受自然灾害地区的供电机构在危机反应、复原和恢复方面经验非常丰富，因为自然灾害是不可阻止的，而且自然灾害的后果也无法预料。

风险管理的另一种形式可能包括考虑定期或经常进行员工背景审查。有效的甄别审查工作

可以预防和阻止员工玩忽职守、偷窃和吸毒，同时可以在雇用新员工、提升员工以及选择承包商和供应商（尤其是那些既在关键设施中工作，又直接支持关键服务的承包商和供应商）时提供参考依据。至于对非本国公民的雇用或使用，可能还需要考虑其他方面的问题。

### 复原和恢复

本“行动方案”的复原和恢复部分是指，为从紧急事件发生时刻起的应急管理、将系统恢复到正常状态、模拟演习、探索经验教训和共享最佳实践方法等工作制定计划。复原和恢复工作因物理和电子资产的差异而存在很大差别。

针对物理设施的孤立有意攻击造成的后果与自然灾害的后果只是稍有不同。类似性体现在受损的性质和立即恢复运转能力的要求上。然而在自然灾害与针对物理设施的计划周密、协调一致并且波及面极广的有意攻击之间有着巨大差异。例如，攻击者可能会同时对若干个最难防御或最难恢复的目标下手。然而，与电子系统安全测试恰成对照的是，物理系统安全测试有一套成熟并被广泛接受的技术。人们常常运用桌面演练的方法为应对自然灾害制定计划。实践证明，这些技术在测试反应和恢复程序方面十分有效，因此也适用于安全问题。

大多数供电机构依赖计算机化系统实现制单、运转和内部管理功能。竞争激烈的电力市场需要通过电子交易系统完成投标和报价，因此依赖性很强，对时间的要求也很高。制定一项将遭破坏的电子系统恢复正常运转的计划很可能会决定商业运作的成败。行之有效的复原和恢复计划需要周密考虑发生各种攻击的可能性。电子犯罪可能需要其他特殊处理手段，如出于执法目的保存计算机证据等。这些调节也可能会影响服务或设备的及时恢复。

### 监控和更新

监视和记录系统可以标识出可疑和实际发生了的意外事件，以供追踪调查。实时监控可使机构对物理和电子威胁及时做出反应。及时的监控和反应是保持运转完整性和可用性的关键因素。

物理安全实时监控工作涉及的范围相当广泛，可能需要考虑登录控制系统报告、视频监视、语音记录、设备检查、职员的可靠威胁报告、执法机关的外部威胁报告等因素。

供电和配电机构可能需要将来自若干不同日志源的独特事件联系起来加以考虑，从而判断那些单独看或许不成为威胁但结合到一起却表明某种特定有害威胁 / 事件的类型。信息源的数量和潜在的大量日志数据可能要求具有自动实时监控和报警功能。

负责分析监控信息的单位可能需要向企业管理层、内部安全部门和若干外部组织如 NIPC 和执法部门报告所发现的威胁问题。供电和配电机构可以考虑通过电力工业可靠性计划（如电力部门“信息共享和分析中心”）以及电力工业-政府部门合作计划（如迹象发现、分析和预警计划）与相关各方交流报告内容。

### 信息共享、教育和认识

电力行业组织对紧急事件的全面反应在一定程度上依赖于有关威胁和脆弱性信息的及时共享。50 多年来，电力行业的报告和报警渠道得到了很好的发展。由于人员和物理基础设施都是现成的，在业内就影响电力系统可靠性的电子和物理安全事件建立信息共享和事件报告机制完全可以在现有的结构和程序上进行。以下几项安全事件报告方案正在实施之中：

- NERC 的“可靠性认证信息系统”已扩大到应用于报告电子事件。
- NERC 和国家基础设施保护中心建立了“迹象发现、分析和预警”报告和报警系统。

该系统可以将事件报告传递到 NERC 的电力部门信息共享和分析中心（ISAC）或联邦调查局的国家基础设施保护中心（NIPC）。这些渠道还可被 ISAC 和 NIPC 用来向业内成员发布预警通报。

- NERC 负责关键基础设施保护信息系统（CIPIS）的管理工作，以用于不可控空间通信。
- 业界成员可以单独按照自己的选择参加联邦调查局的“InfraGard”计划或私营行业现有的包含报告和预警机制的其他信息共享计划。
- 所有与国土安全部有联系的关键基础设施部门都目前都在审定标准化威胁报警级别。此外，电力部门的组织正在为每个报警级别制定反应指导方针，其中阐明了应该积极采取的应对预料威胁的行动。
- 电力部门信息共享和分析中心与其他基础设施部门（如天然气、石油、化学部门）的信息共享和分析中心携手合作，共同确保安全事件和预警通报信息的有效跨部门交流。

提高员工安全意识以及加强对电力行业领导层、操作人员和安全专业人员的培训，是应对电子和物理安全问题的一个重要手段。企业的最佳防御是全体员工都了解和支持安全政策和程序。提高员工安全意识的计划应该教育员工行动时切记减少安全风险。例如，必要时选择、保护和改变“好”口令，不增加未经授权的调制解调器，切碎可能危及安全的文档，提高员工对社会工程风险的认识等。NERC 和爱迪生电力研究所正在为电力行业制定一系列自愿性安全指导方针，其中阐明了可用来保护电力基础设施系统的总体手段、注意事项、实践方法、操作和规划理论。

安全问题的解决要求企业及其员工意识、理解和接受问题存在的现实。做到了这一点，随后有关角色和责任、使用工具和实施适宜控制的教育步骤才会被更好地接受和消化。提高认识的教育还涉及把受教育者培养成问题的解决者，使他们掌握现有的知识、技能和创造力，从而从深度和广度两个方面扩大可用资源。

提高业内企业及地区委员会高级管理人员安全意识的工作可以为他们提供额外的信息，使他们在确定和管理不断涌现的风险时能够做出更好的决策。NERC 已经制定了一项专门针对 CEO、CIO、运营经理及 NERC 理事会成员的提高认识计划。

### 电力行业内部的协调

供电和配电机构持续不断进行着合作，发生突发事件时，依靠协调一致的操作系统和共享的资源应付自如。正式和非正式相互援助计划早已存在，其中有些计划是针对特定行业组织的（如爱迪生电力研究所的相互援助计划、针对市政供电机构的联邦反应计划等），另一些计划则是针对特定地区的（如针对东南部供电机构的紧急情况物资互助支持计划等）。此外，NERC 维护着一个北美地区大型电力系统备用变压器数据库和一个大型供电和配电设施名称和合同数据库。

### 互依赖性

基础设施的互依赖性是指关键基础设施内部和各关键基础设施（电力、天然气、石油、煤炭、电信、银行与金融、运输、供水系统、应急服务、政府运作、制造业以及食品 / 农业）之间的物理、电子和新经济（电子商务）连接。这些连接在规模和复杂程度上差异很大，通常涉及大量系统成分。

从本“行动方案”的这个因素看，连接的确定和分析要求对每个基础设施成分以及相关系

统是怎样相互依靠和支持的都有透彻的了解。此外，并非基础设施的所有方面都是互相依赖的，对于这点，可能需要认识、了解和做进一步研究。

例如，大多数新建发电厂要依靠天然气，而天然气本身可能要依靠电力驱动控制系统、管理存储操作和运行压缩站等，同时要依靠电信系统传送操作信号。

电力部门在北美部分地区有着标识和应对地方和地区级互依赖性的丰富经验，进一步加深对地方、地区级和跨行业相互信赖性的了解的工作已经在关键基础设施安全合作组织（PCIS）的介入下展开。

### 研究与开发

为了更好地应对国家关键基础设施面对的新挑战，需要加大研究开发的力度。这些挑战涉及物理和电子信息安全，也包括产生于基础设施内部的不断发展变化、日趋复杂的互依赖性的威胁。迎接这些挑战需要新的资源，需要对安全模式（避免、保障、检测和恢复）的研发需求和差距以及政府、业界以及学术界之间的新合作方式有一个全新的审视分析。

与程序控制系统（SCADA、EMS、DCS、PLC 和智能现场设备）相关的安全问题显示了潜在的研发机会。为信息技术应用而设计的加密技术、防火墙和入侵检测系统不能很容易就兼容到程序控制系统之中，而后者则需要快速反应速度和应用各种通信协议。这种情况要求对技术和理念的局限性有进一步的了解，从而开发出解决这些问题的新方法。

### 与 CIP 相关的法律问题和挑战

为了确保北美关键电力基础设施的安全，政府必须与需要得到合作和信息共享帮助的电力部门共同加强以下方面的工作：

- 根据《信息自由法》（FOIA），美国政府行政机构和部门拥有的记录应该供公众读取。然而，国会意识到某些信息的公开需要得到合法限制，同时出于协调各项法律法规的目的，国会规定了有些信息不予对公众公开的多种豁免例外。当前，现有的任何 FOIA 豁免例外还不足以保护威胁和脆弱性信息不被泄露。
- 企业需要避免在关键信息共享方面受联邦和州反托拉斯法律的无意限制。联邦反托拉斯法律和政策旨在促进市场竞争。业界参与者之间的某些类型的协议、合作安排和信息共享可能具有反竞争效应。这些反竞争效应可能存在于那些会造成提升价格或减少产量（且不论意图如何）影响的协议（或合作模式）中。各市场中大集团之间的合作可能会引起未参与合作的市场成员、机构和其他非政府组织的质疑，从而增加参与者的风险。
- 企业需要避免承担由各种风险管理规划活动，如风险评估、基础设施安全检验或某些威胁和脆弱性信息的共享带来的法律责任。需要解决的问题包括：定义管理人员、董事和官员的责任；限制关键基础设施设备所有者/运行者的责任；推动实施支持电子安全/责任保险有效性的战略；制定破坏防范措施以防连锁性影响造成的冲击；限制由对全国性或全球性公司提出的前后不一致要求带来的责任。
- 电力组织的电子威胁防范开支需要在联邦公司所得税方面得到一致的优惠待遇。特别是，是否允许公司开支这笔钱，或者是否要求公司分批支出这笔钱，即便公司不想这样做。只要这方面的支出在公司承受能力之内，它们是愿意承担的。特别是在某些时候，如果政府当局出于某些原因要求公司将电子威胁防范水平提高到超出公司管理层

或董事会对被要求的信用责任的设想，情况尤其会如此。如果政府要求业界增加安全开支，那么把纳税优惠待遇作为政府政策的一个组成部分而不是相反，或许是达到这个目的的一条途径。

## 5. 总结

新技术的应用以及世界政治和社会的不断变化，增加了威胁和脆弱性，其中既有物理的也有网络的，网络又包括电力网和电子网。而可靠服务所受到的威胁，其性质和程度又因新的和不断发展的国家和国际紧张局势而被进一步加大。2001年9月11日对世贸中心和五角大楼的恐怖袭击对维系我们生活各个方面的服务和系统产生了深远影响。正如商务部关键基础设施保障局最近指出的那样：“电信服务遭受的损失阻碍金融交易服务的展开，同时阻碍电力的传送，这已经不再是演习中的场景。可以这样说，没有‘e’电，也就不可能有电子商务。”

出于公司运营的合理要求，同时也出于国家安全的考虑，单个机构应该通过管理和适当保护其自身的系统以及各实体之间的连接来对付这些威胁，从而确保北美电力传输系统的可靠性和完整性，以及维持公众对供电机构的信心。对供电和配电系统所面临的风险的评估应该考虑各实体及各部门之间的互依赖性，而强化的保护工作应该考虑如何加强各实体及各部门之间的合作。

综上所述，本“行动方案”将有助于维护电力行业的安全、用户的信心以及普通公众对北美电力供应和传输系统的可靠性和完整性以及电力基础设施的信心。



---

## 十五、保险部门对保护网络空间的国家战略 的响应 v5.1（摘要）

美国保险部门

---



扫二维码阅读全文

## 1. 保险部门简介

保险部门，具体而言是指那些针对“网络损失”提供保险业务的保险商，在保护国家关键基础设施远离网络风险方面担负着重大使命。它们不仅帮助公司免遭严重运行和金融危害，而且在教育和激励公司减少潜在灾难性网络损失风险方面发挥着不可替代的作用。对于当今依赖计算机系统才能正常运转的经济活动，以及避免承受不该承受的负担的纳税人（他们可能会被要求出力拯救濒于破产边缘的公司）来说，防范和减少网络损失，尤其是破坏关键系统或众多公司网络的严重事件所造成的损失，非常必要。

在帮助公司评估和管理多得令人难以置信的大范围风险方面，保险部门具有多年的丰富经验。例如，该部门技术专家提出的实践方法帮助降低了工作场所人员伤亡、汽车事故、与产品相关的消费者伤亡等多种风险。保险公司还在环境和与雇用相关的法律义务等众多方面提供了管理责任指导。由于保险商与客户关系密切且保持着日常性联系，同时收集有客户以往损失的数据，它们往往是损失脆弱性最新模式的第一见证人。因此可以说，保险商是通过普遍教育和提高安全意识计划以及专为特定公司客户设计的培训计划而开发和推广新的最佳实践方法和标准的首批参与者之一。

至于那些以出色的风险管理计划和标准减少了其网络损失事件中的脆弱性的公司，在遇到其他类型风险时可以获得选择更好的保险产品、较低的保险费用以及其他优惠保险条款和条件等方式的回报。这有助于降低公司的风险成本，避免与财产损失方、愤怒的利益相关人和监管机构对簿公堂，乃至全面提高公司的运行效率。公司一旦改善了自身的风险防范状况，就会在利益相关人和贷款方眼中成为更好的投资对象。

然而不幸的是，无论公司在信息安全上进行多大投入，它们也依然无法万无一失地保护自己免受黑客、犯罪分子和恐怖分子选择对公司电子商务和信息系统发动的攻击。这些人会不断想方设法潜入和篡改公司的系统。公司建立和安装新型安全系统后，他们马上就会找出办法躲过监视。尽管公司不在全系统上投资是愚蠢的决定，但是它们宁愿显得愚蠢也不愿意配置了安全网后安全事件仍然时有发生。

应运而生的网络保险产品将从金融角度提供一种机制，确保公司在灾难发生后尽快继续运营和业务操作。除此之外，保险商还能运用其专业经验帮助客户针对灾害制定计划并迅速实施这些确保业务不中断并在必要时恢复的计划。

美国面临的国际国内物理及其他网络威胁没有一丝减弱的迹象。普遍性网络威胁的愈演愈烈已经促使保险和再保险部门把工作重点放到有关网络威胁的教育与提高意识项目上，同时就高级网络风险管理的技术支持提供指导。所强调的风险管理决策的重要方面如下：

- （1）确定和评估电子商务活动给公司带来的风险和潜在影响。
- （2）确定运用传统保险产品应对这些新的或强化了的风险时所会遇到的常见障碍。
- （3）借助网络风险评估程序支持决策，以减少已知脆弱性，防范有可能破坏业务活动或危害公司财政状况和声誉的威胁。
- （4）确定如何通过购买专项网络风险转移保险产品为公司提供必要的财务平衡保护。
- （5）制定和实施业务连续性计划，其中包括对是否购买可以提供实施计划所需资金的网络风险转移产品进行决策。

对于很多保险商来说，网络保险目前依然是一个回报颇丰并且持续增长的市场。然而有若干障碍妨碍了它以应有的速度快速发展，其中包括：①对保险的价值意识；②一个能够支持保险产品的规模可观的再保险市场；③能够对网络风险暴露程度进行定价和建模的可用数据。由于存在这些障碍，本文就保险部门应该采取的行动提出如下建议。

#### 部门行动建议一

保险部门应该考虑提供专业化网络保险产品。

这些产品通常包括，针对如何减轻网站、系统和数据遭破坏、毁坏或拒绝服务以及由此产生的司法诉讼所造成的金融影响提供广泛的金融风险损失转移保护。这些产品还可以为网站、系统、数据和危机通信服务的事发后修复和重建提供资金，从而恢复消费者、员工、利益相关人和其他投保公司利益相关人的信心。最后，保险商在考虑提供这类保险业务时应该考虑整合可用的损失防范服务。具体而言，这些服务应包括以下内容：

- 评估和了解：对现有过程、程序、人员、技术和网络金融管理状况进行分析和评估。
- 损失防范、教育、意识与业务恢复：采取积极措施增强客户戒备、抵御网络攻击以及在企业和系统遭受广泛和系统化网络攻击后从财政和技术两个方面迅速恢复的能力。
- 检测和反应：在技术工具、软件、数据、关键基础设施、私有网络配置和知识产权等方面制定和实施针对网络攻击的检测、早期预警和事件反应战略。
- 重建和恢复：保险和再保险部门在出资帮助客户在将技术和金融服务功能复原和恢复至正常运行状态方面发挥关键性作用。
- 金融风险管理：保险机制为客户提供财务平衡保护，从而帮助客户应对网络攻击导致的意外重大金融灾害。

#### 部门行动建议二

政府应该鼓励运用保险和其他风险管理技术来减少私营部门网络损失的风险以及减少网络攻击发生后的金融损失。

应鼓励其产品或服务对国家经济、公众健康、社会福利和公共安全具有直接或间接影响的公司购买实力强大的保险商的特定网络风险保险。

#### 部门行动建议三

通过公共和私营部门之间的合作展开提高安全意识活动，对公开交易企业的董事会成员、行政官员和重要利益相关人进行教育。

董事会成员应像在“千年虫”危机中所表现的那样积极介入网络风险的管理工作。没有公司董事会的主动参与，美国关键基础设施的安全就无从谈起。

#### 部门行动建议四

通过政府行政和立法机关之间的合作消除法律和经济障碍，进而加强公共与私营部门之间、各私营部门之间以及私营部门内部的信息共享，这是确保国家网络空间和关键基础设施安全的关键所在。

这些障碍包括《信息自由法》（FOIA）应用于公共部门信息共享的可能性、联邦和州反托拉斯法律应用于私营部门公司之间信息共享的可能性以及泄露此类信息引起法律责任的可能

性。针对“千年虫”问题通过立法法案的经验对此尤其具有借鉴意义。因此，应敦促国会就《信息自由法》、反托拉斯法以及相关责任问题通过与“千年虫”法案类似的立法法案。

### 部门行动建议五

公共-私营部门应通力合作，共同出资开发数据和风险模型，以量化和控制网络风险，从而使保险商得以恰当定价和提供网络保险产品。

对于保护保险商免受产生于一个或多个保户大规模网络风险的金融冲击的再保险商来说，这方面的信息至关重要。如果没有针对网络风险的强有力再保险市场，保险商要么会拒绝进入网络保险市场，要么会严格限制其网络保险业务所涉及的范围。

对网络风险的量化是在已知网络脆弱性导致的可预料损失与无法预料、非经常性并且有可能产生灾难性和系统性损失的网络事件之间有效分配资源的关键。

对网络风险损失事件造成的经济后果进行量化，会为将稀缺的国土安全资源能够有效配置给这些会对经济和国家安全造成威胁的非经常性、无法预料事件创造出机会。

因此，国会应该为相关联邦机构提供足够的资金，以制定连续收集数据程序和推动网络安全风险和风险管理领域的研究与开发。

尽管大量可用数据散布于政府庞大的基础设施之中，但政府也依然称得上是一个大数据库，因此，为了挖掘现有数据的深层价值，政府必须与保险商和其他私营部门参与者密切合作。将这些数据进行挖掘整理之后，政府可以借此协助保险商开发出一种针对网络风险的建模方法。该方法与已被保险商和再保险商开发出来用于传统物理危险的风险建模方法类似。“9·11”事件之后，有限的技术资源已经转向对物理恐怖袭击的突发性关键风险进行量化和建模，这种政府方面的帮助就显得更加重要。

### 部门行动建议六

联邦政府应与保险部门共同鼓励展开教育和提高安全意识活动，以加强相关人员对网络风险和强有力的网络风险转移保险市场的价值的认识，从而使之在政府支持下更快地发展。

因此，应该敦促政府的行政和立法机关在适当的时候以适当的方式对网络保险市场给予支持。

## 2. 总结

保险与再保险部门可以借助联邦政府与各关键基础设施部门持续不断的合作，集中精力全面实施上述部门行动方案。

我们相信，政府机构可以通过鼓励公开交易公司董事会和管理人员持续并积极关注网络安全管理，使公司最高层树立对网络安全问题的正确认识。我们还相信，在技术对于商品和服务的提供显得越来越关键的情况下，竞争性保险市场机制将会给高度重视网络风险管理的私营公司日渐丰厚的回报。

我们确定了实施这些部门行动方案的以下四个基本原则，用以指导保险和再保险部门在支持实现国家安全和经济稳定目标的过程中努力减少和转移网络风险：

- 保险和再保险部门，具体而言，是这些部门中与客户、经纪人和政府进行协作并开展网络风险保险业务的部分，应对那些造成损失和破坏服务，且可能具有进一步灾难性

系统风险的网络威胁和已知脆弱性进行确定和评估。

- 国家关键基础设施以及其运营业务会对公众健康、社会福祉或经济活力产生直接或间接影响的公司的所有者和运营者应该通过合理的风险管理措施、业务和安全实践方法，以及通过制定综合了最佳风险保持、风险缓和和风险转移级别的行动计划，参与到持续高水平保障基础设施安全的工作中去。
- 应对国家关键基础设施所有者和运营者施以鼓励，动员他们防范包括有组织的网络恐怖活动在内的各种系统性网络风险。
- 在必要的情况下，联邦政府应与我们的客户（所有者、运营者和其他第三方服务提供者）协同合作，防范和应对危害国家经济稳定的系统性网络攻击。

本框架反映了保险和再保险部门的持续工作重点。作为一种市场驱动力，该部门在教育、鼓励和奖励合理业务实践措施、信息安全原则和高级网络风险管理政策方面发挥着重要作用。

---

## 十六、供水部门关键基础设施保护国家计划 (摘要)

美国供水部门  
2001 年 7 月 23 日

---



扫二维码阅读全文

## 1. 引言

根据克林顿政府第 63 号总统令，供水部门与电信、能源、银行与金融、运输、应急服务等其他部门一起，被指定为关键基础设施。饮用水的持续有效供应是保障我们国家公众健康和经济繁荣的一大基本要素。美国的供水部门由成千上万单个供水系统构成，其中有的为不到 100 人服务，有的为数百万人服务，规模各异。系统的归属也差异很大，其中有的是市政所属系统，有的则是私营或归投资人所有。

在历史上，关键基础设施一直被视为是相互之间没有什么依赖关系的独立的物理或后勤保障系统。随着信息技术的迅速发展以及对提高效率的要求越来越高，关键基础设施已经变得自动化程度越来越高、相互之间联系得越来越紧密。这些发展同时也使基础设施在面对设备故障、人为错误、天气和其他自然原因以及物理和网络攻击时显得非常脆弱。我们的经济越来越离不开相互依赖且依靠网络支持的基础设施。对国家基础设施和信息系统的攻击很可能会导致对美国公众健康和经济稳定的巨大伤害。

供水部门面对攻击，其中包括对供水量、水质以及针对供水系统的计算机系统的攻击时，也十分脆弱。对水源（如水管入口、泉源）、水处理厂（如电源、管道、水泵和水处理设备）、储水设施（如水塔、水泵和泵站）和送水系统（如管线和送水渠道）的破坏，会造成供水中断。物理威胁还包括供水的潜在化学或生物污染以及其他水质问题。网络威胁对象包括用于通过监控和数据采集（SCADA）系统监测和控制水质和水流的计算机操作。SCADA 系统极易受计算机黑客影响，从而有可能造成水质变化、供水流速变化或面向用户的“拒绝服务”。心怀不满的员工、蓄意的破坏分子、别有用心的组织以及怀有政治目的的恐怖分子是最有可能的犯罪者。

此外，饮用水与公众健康密切相关，它是公众关心的敏感问题，这也是供水系统多少有些独特的地方。与其他关键基础设施部门一样，供水系统必须应对任何因破坏或污染造成的意外中断的影响。然而，供水系统又与其他关键基础设施不同，即便中断故障被解决、全面服务被恢复，公众的信任问题依然会久久挥之不去。出于这一原因，某次对系统的袭击威胁即便没有任何明显的行动，也会对供水系统产生影响。

当今的供水系统与其他关键基础设施不可分割地连接在一起，充足和优质的供水是保持经济正常运转的关键。水的处理和配送依赖于可靠和高质量的电力。供水系统内部的监视和控制系统与电信部门紧密相连。大坝可以提供水源，同时还能发电。这些方面的高度连接和相互依赖给所有供水系统带来了脆弱性。运输系统为水处理所需的化学制剂提供了输送渠道，同时也为进入广袤分布的供水运营中心提供了通道。水是消防应急响应部门的关键要素。

第 63 号总统令将供水工业确定为八大关键基础设施之一，要求确保其物理设施和计算机系统的安全。该总统令阐明各级政府和私营部门必须通过协调一致的合作共同解决与关键基础设施保护相关的问题。总统令出于推动协调和合作的目的，要求公共-私营部门通过建立合作伙伴关系来增强关键基础设施抵御威胁的力量。

## 2. 供水部门的代表

美国环境保护局（EPA）是负责供水部门的联邦领导机构。EPA 指定大城市水工业协会（AMWA，代表了大城市的供水系统）为供水部门领导机构。其他代表供水系统或其利益相关人的组织还有美国水工业协会（AWWA）、供水公司全国协会（NAWC）和 AWWA 研究基金会

(AWWARF) 等。

### 3. 顾问组

为了履行自己在供水部门的领导职责，AMWA 于 2000 年 12 月组建了供水部门关键基础设施保护（CIP）顾问组。该顾问组致力于协调供水行业内与基础设施安全相关的活动。顾问组由来自 AMWA、AWWA、AWWARF、NAWC 和州饮用水管理机构协会、政府参与者（EPA、联邦调查局和教育部）的代表组成，自 2000 年 1 月起每月召开一次会议。

顾问组最初的会议主要致力于熟悉和了解需要由其参与解决的安全问题。此外，顾问组从 EPA、联邦调查局、关键基础设施保障办公室（CIAO）、其他联邦机构和执法机关得到了很多有关安全问题的最新资料。顾问组将着重解决的几个具体问题包括供水部门信息共享和分析中心的角色、《信息自由法》（FOIA）问题和供水系统的人员培训需要。

### 4. 信息共享和分析中心

第 63 号总统令还鼓励每个关键基础设施均建立私营部门信息共享和分析中心（ISAC），用以收集、分析、整理和传播有关威胁、攻击、脆弱性、异常情况和安全实践方法的信息。有关供水系统所受威胁和攻击的信息及其脆弱性和相关解决方案的积极和及时交流，是保护供水系统的关键所在。信息共享的目的是帮助供水系统更好地保护自己、提高执法效率和改善国家安全状况。

AMWA 负责供水行业的 ISAC 建立和发展工作，并且已在技术手段方面做好了准备。这些准备工作涉及了三个具体目标：①评价 ISAC 选择方案；②建立 ISAC；③就脆弱性评估和 ISAC 程序培训供水系统人员。AMWA 已向 EPA 提出了拨款申请，请求 EPA 为 ISAC 的建立提供资金方面的协助。ISAC 建立的具体时间表尚未确定，但初步时间定为 2003 年年初。

### 5. 供水部门的问题

供水部门顾问组在最初的几次会议上确定了与供水行业基础设施保护相关的若干个问题，其中包括以下几个。

- 了解问题：供水部门没有为以往的威胁和事件建立过数据库或没有整理过相关信息。有关已知威胁和事件的文件对于供水系统的人员教育有很大的帮助作用。此外，有关已知威胁和事件的信息还可以用来帮助确定应对威胁还需要加强哪些安全措施，同时还有助于判断安全开支的合理性。
- 物理和网络威胁：供水部门与其他民生工业部门一样，受到了网络 and 物理攻击的威胁。供水部门需要付出努力来应对这两类威胁。
- 互依赖性：供水部门与其他关键基础设施部门之间存在着若干种互依赖性。这些互依赖性给供水部门带来了许多脆弱性。
- FOIA：很多供水系统归城市地方政府所有，必须遵守州《信息安全法》（FOIA）的要求。安全工作也必须符合 FOIA 法律规范。因此，在当前情况下，像具体描述了供水系统脆弱性的脆弱性评估这样的敏感文件无法摆脱 FOIA 的要求而受到专门保护。



---

## 十七、铁路部门关键基础设施保护国家计划 (摘要)

美国铁路部门

2002 年 6 月

---



扫二维码阅读全文

## 1. 行业概述

美国的铁路部门由私营部门经营已有约 175 年。铁路公司拥有通行权，需自行铺设和维护铁路线路，同时拥有机车和大部分所需车辆。铁路公司还拥有和运行着自己的火车调度和信号系统。

美国的货运铁路负责国家 40% 以上的城际货物运输，其中包括火力发电厂所需煤炭的 64%、国计民生所需粮食的 40% 以及水处理厂所需氯和制药厂所需化学制品的绝大部分。国防部指定 3 万多英里铁路走廊为国防基本线路。这个战略铁路走廊网（STRACNET）是国防部运输军用物资的基石，尤其是在有大规模军事调动的时候。美铁（全国铁路客运公司）则提供全国铁路客运和邮政及快递服务。

作为一种网络工业，铁路有着业界密切合作的悠久历史，从部门创建之初就采用了标准轨距和通用设备。早在 100 多年前，铁路行业就制定了一项安全要求：所有需要在各铁路公司之间交换使用的车辆都必须在设计上符合本行业一个机械委员会做出的规定。因此，经营交换服务的车辆所有者必须遵守“交换协议”规定的技术规范。该“交换协议”还要求其他旨在确保铁路服务安全高效运行的协议必须满足国家的经济和军事需要。美国、加拿大和墨西哥的各大铁路公司都是这项协议的签约者，从而构成了庞大的北美货运铁路网。

各铁路公司之间的合作是日常工作的需要。而在发生地震、洪水、塌方、暴雪等各种影响物理基础设施的自然灾害期间，这种合作显得尤为关键。本行业制定了涉及范围很广的火车意外事件应急反应计划，其中包括危险材料运输的应急反应计划。各铁路公司的政策执行人员（通常由联邦政府委任）负责协调各公司之间以及与州和地方警察机关、联邦调查局之间的合作活动和信息共享。

铁路行业从初期采用电报系统起就开始涉足信息技术。30 年前，铁路部门创建了一个货车信息中央交换站，所收集的信息可通过现代通信系统传递给所有铁路公司。即便是今天，也没有几个行业能在计算机化程度上与铁路部门相比。信息技术和现代化通信系统是铁路高效运行和提供客户服务的基础和关键。美国的铁路被视为世界上最佳货运铁路，信息技术的有效运用是赢得这种赞誉的原因之一。

## 2. 现任部门协调员的活动

根据第 63 号总统令和美国交通部的要求，美国铁路协会（AAR）<sup>①</sup>同意担任负责关键信息系统保护工作的铁路部门协调员。AAR 的成员包括所有在美国境内运营的一级铁路公司，它们的年总收入至少为 2.585 亿美元。加拿大和墨西哥的主要货运铁路公司和美铁也是 AAR 的成员。

为履行作为部门协调员的职责，AAR 创建了地面运输信息共享和分析中心（ST-ISAC），参与者可以匿名或署名两种方式自愿向中心递交有关信息系统脆弱性、突发事件、威胁和解决方案的信息。此外，ST-ISAC 的参与者还可取用由政府 and 世界各地商业信息服务机构提供的具

---

① 最新的美国货运铁路工业统计数字显示，在铁路部门中，AAR 成员经营的铁路英里数占 76%，雇用员工数占 91%，货运收入之和占 97%，货运量之和占 97%。

体威胁信息。

ST-ISAC 于 2002 年 3 月 15 日开始运行，以网络和物理威胁、脆弱性和解决方案信息交换站的形式提供相关服务。AAR 目前正致力于邀请经营其他地面运输模式的公司也加入 ST-ISAC，它的目标是把所有相关实体（其中包括市郊铁路运输经营者）全部吸收到 ST-ISAC 中来。

### 3. 铁路部门对“9·11”事件的反应

“9·11”恐怖袭击发生后，AAR 成员立即采取了 30 多项措施确保业界安全，同时保持了自身支持国家经济、国防和公众健康的能力。例如，铁路公司加强了全系统的安全检查工作。重要铁路设施和信息已经被限制进入。业界增加了网络安全程序和技术手段。员工档案都要送交联邦调查局与恐怖分子名单核对。安全汇报已经成为每个员工日常工作的一个组成部分。

AAR 组建了一个铁路安全工作队，直接归 AAR 主席 / CEO 领导，运用中央情报局和其他情报部门的“最佳实践方法”，负责对本行业进行全面风险分析和制定安全计划的工作。AAR 组建了 5 个关键行动小组<sup>①</sup>，由 150 多位经验丰富的铁路公司人员、客户代表和情报人员组成，分别从以下五个方面对铁路部门的资产、脆弱性和所面对的威胁进行分析研究并排列工作重点。

#### 信息技术与通信

该小组分析研究了本行业通信、控制系统和信息系统的状况，其中包括评估与系统备份、数据保密、紧急事件处理和服务恢复相关的程序。很多新的安全措施很快就要在全行业落实实施。

#### 物理基础设施

该小组评估了关键桥梁、建筑物、调度中心、隧道、仓库及其他设施的物理安全状况。一个关键资产数据库已被建立并登录在一个地理信息系统之中。该小组还着重强调了跨国界和端口“关”的物理安全问题。

#### 运行安全

该小组定义了“列车生命周期”，确定了如何将运行中的列车遭计划外损坏的可能性降到最低的方法。它还着重研究了燃料供应问题。

#### 危险材料

该小组分析研究了危险材料的铁路运输问题，重点是潜在安全风险最大的有毒气体等材料。该小组为这些材料确定了当前所应采用的运输方式，并与化学工业以及罐车制造厂家共同评估了各种选择方案，其中包括限制运输线路、对产品进行再制造和包装等。

#### 军方联系人

该小组与国防部及其所属军事运输管理司令部合作，共同提出了应立即并持续实施的军事运输规定，确定了业界应在货运量、安全和设备等诸多方面满足军方的需要。

---

<sup>①</sup> 美国公共运输协会、联邦铁路管理局和联邦运输管理局目前的一项联合行动在着重研究有关铁路客运的问题。

铁路公司和行业协会的最高层官员参与了这一风险分析过程。各关键行动小组分别由一位铁路行业副总裁级官员领导。这些小组领导人每周要通过电话会议向 AAR 董事会汇报工作。产生于这一过程的“恐怖主义风险分析和安全管理计划”是一项横跨多项内部职能、重点突出的行动计划，所涉行动都是加强国家货运铁路网的安全和提高铁路部门支持国家经济、国防和公众健康的能力的关键所在。ARR 董事会于 2001 年 12 月 6 日批准了这项计划。计划提出的安全程序和分析结果（包括具体行动和措施）将定期接受效果评估，以确保实现安全技术和程序成果的最大化。

## 4. 恐怖主义风险分析和安全管理计划

铁路行业的这项计划定义了四个戒备级别，详细阐明了随恐怖主义威胁程度的增加而逐步升级的每一级戒备所应采取的行动。各级戒备的行动说明中包含了用于各个运营方面（包括运输、工程和机械）的应对措施、信息技术 / 电信和铁路政策。

### 一级戒备

被定义为“新常规日常操作”，用于出现一般性潜在恐怖主义活动威胁的时候，但只能保障常规安全状态。恐怖主义攻击的性质和范围难以预料，一般性情况也无法证明需要全面采取更高级别的戒备。这级戒备涉及了 33 种行动，其中包括：

- 开展安全培训和提高人员安全意识活动。
- 确保信息不泄露给任何不相干的人员。
- 封锁未经授权者对某些危险材料、军用物资、核燃料和其他敏感材料运输过程的接触和跟踪。
- 定期检测安全系统的运转是否符合要求。

### 二级戒备

被定义为“提高安全意识”，适用于出现针对铁路人员和设施的一般性非特定潜在恐怖活动威胁的时候。遇到这种情况，铁路部门要处于二级戒备状态。这级戒备增加了 20 种行动，例如：

- 每日工作汇报中必须包含安全和意识的内容。
- 对运行中的车厢和集装箱进行货物检查。
- 对归铁路部门所有的机动车辆进行定点货物检查。
- 增强对指定设施的安全保卫。

### 三级戒备

被定义为“针对美国或铁路工业的明确攻击”，适用于出现越来越明确且更为具体的恐怖活动威胁的时候。宣布进入三级戒备状态的决策需根据铁路人员和设施所受攻击的具体情况接受评估。这级戒备增加的 40 种措施必须持续实施若干周，同时又不能给铁路公司及其客户带来不必要的困难或对正常运行能力产生影响。三级戒备措施举例如下：

- 进一步限制物理进入，增强对控制中心、通信枢纽和其他指定设施的安全保卫。
- 开始对燃料库和操作设施进行 24 小时监控。
- 要求国民警卫队对关键资产实施安全保护。

### 四级戒备

被定义为“针对铁路工业的确凿攻击威胁或针对美国的真实攻击”，适用于出现针对铁路

工业的确凿威胁，或针对铁路工业乃至美国国家并造成重大人员伤亡的真实攻击，或其他会对安全运作造成严重隐患的紧急情况的时候。这级戒备的新增措施最长实施 72 小时，到时是否需要继续实施应根据定期评估而定。这些措施包括：

- 禁止非关键任务合同服务人员进入关键设施和系统。
- 在列车接受异常物品机械检查期间加强对车辆及设备的安全保卫。
- 确保对指定设施和建筑的保卫措施连续实施。

三级和四级戒备可在全行业内短期实施，也可用于有情报显示恐怖分子行将对某个具体地点或某列火车发动攻击的地理区域或运输项目（如中西部或危险材料的运输等）。

为了对威胁进行监视并在全行业通报威胁的变化情况，AAR 建立了铁路预警网（RAN）。RAN 的中枢是 AAR 的运营中心，二级戒备状态时，这里动用 24×7 移动通信设备；而处于三级和四级戒备时，则采用更尖端的通信设备。创建 RAN 的最初目的是处理物理威胁信息，如今，RAN 已与前文介绍过的 ST-ISAC 连为一体，用以收集、分析和发布有关关键物理和网络基础设施所受威胁的信息。很多 AAR 和铁路公司官员被配发了安全许可证，而 AAR 的运营中心则配置了一套第三代安全电话单元。为了确保敏感安全信息的保密性和完整性，本行业的电子邮件往来一律加密。

## 5. 联邦政府的参与

以往，铁路行业通过风险分析和安全规划程序与联邦政府相关机构长期保持联系。今天，货运铁路公司依然与美国交通部的情报和安全人员、联邦铁路管理局、联邦调查局、国土安全办公室以及州和地方执法机关保持着稳定的联系。本行业将在以下几个方面继续依靠联邦政府的支持和协助来对关键铁路基础设施实施保护。

### 信息共享

戒备级别的宣布、降低和取消由 AAR 董事会负责。当宣布进入某一级别戒备状态时，各铁路公司应立即采取相应行动。威胁信息（包括情报综述、预警报告和现场报告）将有助于业界慎重决定是否应该宣布进入某一级别戒备状态。前文讲过，铁路部门的很多人员被配发了安全许可证，具有确保通信安全的能力。从联邦政府获得及时、具体威胁信息的需要不能被过分夸大。《信息自由法》和有关法律责任的担心阻碍了业界向政府部门（联邦和州一级政府）交流某些信息。这些方面的法律不确定性问题需要通过立法来解决。

### 危险材料运输的研发和相关法规

铁路业界认为，联邦政府应该资助最敏感的危险材料铁路运输的脆弱性和应对措施评估。此外，交通部的某些法规应该废除，以减少危险材料运输信息的泄露机会。

### 国民警卫队

铁路部门处于最高戒备状态时需要来自国民警卫队的支持。国民警卫队应该用来保卫关键节点，并通过计算机应急响应小组和脆弱性评估小组增强对网络安全的保护。与国民警卫队的合作细节目前正在讨论中。

### 灾害恢复和服务的持续性

如前文所述，铁路部门针对危险材料突发事件和自然灾害、操作和管理备份、铁路员工和公共应急响应人员培训制定了应急响应计划。这些计划和程序全部涉及恐怖分子波及铁路的攻

击。此外，还有以下几个问题应由政府帮助解决以加快灾害恢复的速度：

- 政府应与业界共同确定突发事件期间应由第三方首先恢复的国家重点关键铁路数据系统。
- 政府应对全国性电信网的安全和备份进行分析研究。各大铁路公司都聘用长途通信公司传送语音、数据和调度控制信息。此外，铁路公司应被列到需要重点恢复服务的关键基础设施公司之中。
- 政府应与业界共同探索为关键铁路实施提供固化备份设施的可能性。

## 6. 总结

“9·11”事件以来，铁路行业为确保处于潜在风险之中的国家关键铁路设施和人员得到合理保护、免受恐怖分子威胁付出了坚持不懈和计划周密的努力。货运铁路公司全部加入了四级戒备协议，铁路运输网一旦受到确凿威胁，马上能做出反应。由 24×7 通信网构成的铁路戒备网和 ST-ISAC 可以为全北美铁路工业就物理和网络基础设施所受威胁的信息共享和反应提供一种有效方式。

为了应对、减少和最小化危险和异常事件造成的影响，铁路公司已经制定了长远规划和程序，用以保护其员工和所服务社区的安全，同时确保我们的经济赖以生存的货物的正常流动。然而，恐怖分子针对货运铁路的行动会给美国经济产生巨大破坏，同时也会对国防和公众健康造成负面影响。

联邦政府应该全力协助业界保护关键基础设施免受恐怖分子威胁，以及在恐怖袭击发生后协助恢复工作。联邦政府可以介入的方面包括修改相关立法和法规、开展与高风险危险材料运输相关的研发、审核与国民警卫队支持安全保卫工作相关的公共政策以及确保危机期间数据处理和电信的顺利通畅。

---

## 十八、保护新经济时代石油和天然气基础设施的安全（摘要）

美国国家石油委员会  
2001 年 7 月

---



扫二维码阅读全文

## 介绍

1998 年 5 月，美国总统根据国家日渐严重的潜在脆弱性颁布了一项总统令，其中阐明了有关关键基础设施保护的政府政策。作为对总统令的回应，能源部长要求国家石油委员会（NPC）就“保护美国石油和天然气工业关键基础设施的合作方式”提出建议。

能源部长在 1999 年 4 月 7 日致国家石油委员会的信函中要求：①了解石油和天然气工业面对物理和网络攻击的潜在脆弱性；②就业界和政府应该分别和共同采取什么政策和手段来在攻击下保护自己或从攻击中恢复提出建议。NPC 应能源部长的要求设立了关键基础设施保护委员会。

近 10 年，世界在信息技术和电信（网络）革命的推动下发生了天翻地覆的变化。正因为如此，全世界的各种机构正变得工作效率越来越高、越来越富有生产力。

随着网络系统的广泛使用，它们已经成为关键基础设施不可分割的组成部分。美国也跟世界上其他国家一样，作为其生存之根本的基础设施正面临着越来越严峻的威胁。这些威胁不仅包括自然灾害、人为错误和对物理资产的攻击等传统形式，如今还包括了对当今经济已无法与之分离的网络系统的攻击。

过去，石油和天然气工业对其物理设施实施了有效保护。但是，对于各公司越来越依赖的网络系统，却还没有采取保护手段。石油和天然气工业开展本项研究的目的，就是要深入了解其所具有的潜在脆弱性和开发出消除这些脆弱性的方法。

NPC 的报告建议在石油和天然气工业部门内开展确认和消除脆弱性的活动。它将加强业界和政府对于关键基础设施保护挑战的了解和认识。它分析了新经济环境下企业的运作情况，表明企业必须考虑关键基础设施保护的根本性问题方可赢得最大利益。它提出了石油和天然气工业以及政府必须正视的问题，以及需要双方通力合作方可确保业内关键基础设施完整无恙和持续运转的步骤。

本报告提出的建议具有动态性质，反映了石油和天然气工业在巨大变动中的真实情况。对关键基础设施保护问题的认识也在不断发展变化之中。尽管能源部长的要求信具体阐明了多种攻击形式，但本项研究在范围上大大超出了部长所举的例子，其中涵盖了很多有可能发生的瘫痪情况以及潜在脆弱性。能源基础设施与其他部门的关键基础设施之间存在着不可分割的联系，因此，高屋建瓴地全面认识关键基础设施保护是解决问题的关键。

国家石油委员会认为，本报告提出的部分问题必须得到深入挖掘，而对本报告提出的部分建议，必须进行跟踪调查。NPC 提出本报告，意在为富有建设性的讨论定下基调，同时为下一步在能源工业乃至全国范围内绘制切实可行的蓝图打下基础。

## 1. 新经济环境

人们对石油和天然气工业的认识，大多是“旧经济环境”下的印象。旧经济环境发展了一个多世纪，其间发生了很多重大的社会、经济和技术变化，而石油和天然气工业生存于其中的世界也就是在这些变化中构成框架的。近 10 年，美国经济结构的变化堪称天翻地覆，由此引起了经济运作方式的巨变。在这些变化的作用之下，一个“新经济环境”应运而生。



石油和天然气工业如今所处的世界，由于发生了仅仅在 10 年前还难以想象的前所未有的社会和技术变化而变得更加错综复杂了。要想在新经济环境下的竞争中立于不败之地，石油和天然气工业就必须倚重电子基础设施。本行业保护其物理基础设施的工作长期以来卓有成效。然而，电子基础设施的加入，不仅带来了保护电子基础设施的新问题，而且保护物理基础设施也需要使用全新的手段。电子工具飞速发展着，它们转瞬之间就被应用到了石油和天然气工业的电子基础设施之中。这些变化的速度之快，早把保护关键基础设施的手段远远抛在了后面。要想规避新经济环境下的风险，就需要有一种能够统筹兼顾的全面安全方法，而这种方法的效果离不开政府与私营部门的密切合作。

### 美国的经济结构

当今的美国经济由多种差异很大的结构体系混合组成。位于这个结构体一端的是“旧经济”模式，资本投资的变化迟缓是它的主要特征；而居于该结构体另一端的则是“新经济”模式，快速采用信息和全球化发展是其主要运作成分。虽然在由电子商务驱动的数字经济中运行的业内公司被视为采用了“新经济”模式，但是一般而言，石油和天然气工业依旧属于“旧经济”模式的代表。

今天的美国经济体系已经进入了所谓的新经济环境。

- 今天的经济环境由于变化的迅猛快速而大大不同于以往。
- 当今的一大明显特征是新经济实体通过兼并、合资等手段不断增加，行业内不断涌现通过获取运营设施而进入的新来者。
- 企业扩大了运营地域，往往从地方或地区性公司演变成为全国性乃至全球性企业。
- 企业运营的自动化程度越来越高，其中不仅包括固定地点的自动化，而且包括遥控自动化，这使得在某一地点控制分布范围极广的企业运作成为可能。
- 信息和电信技术的发展影响着新经济环境的每个方面，从而使企业对企业、企业对用户和电子交易等创造性运营模式不断涌现。

这些因素与市场信息的快速传播和高度透明结合到一起，缩小了劳动力队伍的规模，改变了对劳动力的技能要求，使企业运作必须注重时效，同时也极大地增加了各企业之间的相互依赖。

### 石油和天然气工业

国家石油委员会的本项研究着重讨论了石油和天然气部门的基础设施安全问题。近 10 年，石油和天然气工业赖以发展的社会和经济基础深受新兴的电子信息集成和交换技术的影响。

该项技术正在改变石油和天然气公司的运作方式。这种改变主要与信息的随时可获得性、数据的高度透明性以及通信的速度密切相关。以往的很多变化都是依靠重大事件或重大发明推动的，其中有很多经过了漫长时间才渗透到国家和世界的经济领域之中。而信息技术和由此产生的电信革命则在经济界掀起了一场全球性风暴。原先在一定程度上保障经济活动稳定性的国界，如今已不再具有限制作用。原先相对比较易于实施物理保护的信息，如今在可以通过计算机进入全球信息网络的个人面前有了潜在的安全脆弱性。

这些问题已经迅速成为重新勾勒经济图景的因素，它们的高速演变推翻了经济界长期以来接受变化的传统方式。以往那种可以在变化之中提供安全保障的比较缓慢的传统发展节奏，如今已经无法适应时代的要求。要想创造出一个安全的基础设施环境，供未来的经营活动在稳定和相对一致的方式下正常进行，就必须对石油和天然气部门有一种具有创造性的全面认识并采

取相应行动。

技术、全球化、企业和法律法规是推动石油和天然气工业适应新经济环境的重要因素。

### 技术

昨天的技术大多都侧重于勘探、生产、运输、提炼 / 制造石油和天然气及其产品之类的运作功能。而今天的可以概括为电子数据快速收集、电子数据传送和互联网通信的技术却是变换式的。它使“不可能”成为可能，影响了石油和天然气工业的每个方面，创造出一批全新的“游戏者”。

时钟不可能倒转，适于旧经济环境的人员、技能和物理结构业已不复存在，而且在今天的条件下也不可能重新形成。与只需关注物理基础设施的时代相比，当今的网络突发事件会产生远要大得多的影响，也更有可能会带来灾难性的后果。任何人只要手里有一台计算机、一个调制解调器、一根电话线或者一个无线电子接口，就有可能造成价值数十亿美元的破坏。对突发事件的反应变得更加复杂，所涉及的范围更广，所需要的时间也更长。

### 全球化

昨天，我们拥有的只是地区和地方市场。通信速度相对较慢，我们所能取用的信息十分有限，而市场也是缓慢变化的；而今天，随着各国在世界范围的竞争压力下被迫开放各自的市场，市场已经具有了全球的性质。由于信息几乎是可以瞬间得到的，市场也变得更加透明、效率更高，竞争自然也愈演愈烈。

结果，新市场环境下的业内公司始终面对降低成本的巨大压力。为了参与到今天的市场之中，很多石油和天然气公司必须把自己看问题的视角从地方扩展到整个世界，而这往往要求建立起触及范围足够广大的全球性战略伙伴关系。所有这些元素全都离不开电子基础设施。

全球性竞争使从前属于美国的石油和天然气基础设施被非美国公司和政府所拥有，从而给美国经济增加了新的脆弱性。

### 企业

昨天，石油和天然气工业相对比较稳定，由大型跨国公司和小规模独立公司构成。员工对企业忠心耿耿，能够长期为企业服务，因此都是经验丰富的“老手”。而今天，大规模的兼并、结盟和合资使企业的性质大大不同于以往。这些在电子技术推动下的变化使虚拟企业应运而生，大大削减了企业的人员，也衍生出了很多全球性企业，同时还使企业发生了服务性转变，打破了传统的石油、天然气和电力公司界线。结果，经济环境变得不再像以前那么稳定，压力越来越大，知识和经验变成了“外部资源”，而“社会”雇用合同也不复存在。

由此带来的后果是，劳动力不再像以前那样忠于某一具体企业。这种情况再加上员工对供职企业不甚了解，使企业员工有意或无意破坏关键基础设施的可能性大为增加。经济实体的相互依赖和电子信息的流动又使这样的破坏有可能造成巨大影响，同时也削弱了企业及时处理危机的能力。这种以前并不存在的依赖性和互依赖性已经形成，增加了企业所处环境的复杂性，同时使基础设施暴露在更大的风险之下。

### 法律法规

昨天，法律可以着重处理石油和天然气业运行的细微问题，业内游戏者都被精确界定，而

一个世纪的经验也使明确的规矩得以有效实施；而今天，法律已经远远落在了由新经济环境带来的变化后面。此外，欧盟、北美自由贸易联盟之类机构的出现使法律法规有了涉及范围更广也更复杂的视角。外国政府对从前属于美国的公司的参与带来了主权、纳税制度和合同法之类的新问题。法律法规必须关注的新方面每天都在出现，例如，“爱你”病毒的始作俑者在菲律宾法律下就不会被起诉。这种情况尽管并非完全没有先例，但是这些变化的发展速度最终会给社会带来巨大隐患。

面对这样的情况，政府管理者和立法者往往倾向于“减缓”这一发展过程。结果可能是仅仅由于新情况的复杂而使法律法规在地方、州、全国乃至国际层面上发生冲突。法律法规缺乏确定性和界定含混，会导致电子系统更易受无意或有意入侵的破坏。

### 发现和结论

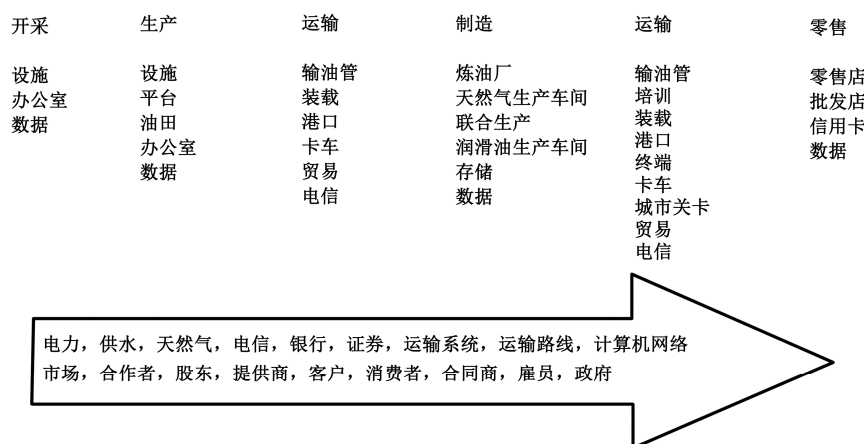
- 社会已经从渐进的变化模式转向了以过去难以想象的速度激变的模式。
- 市场或服务于市场的企业正在变得越来越具有全球化性质，而且结构体系也变得越来越复杂。电子通信和信息技术的广泛应用已经使一切都成为可能。
- 为了在竞争中求生存，业界参与者正在变得越来越依赖于电子系统。因此，快速的变化预计还会继续，而且变化的速度在未来可能还会加快。
- 由于在全球化的推动下电子通信和信息技术被越来越广泛应用，石油和天然气工业也在发生变化。
- 由于企业结构日趋复杂、员工人数比以往大为减少，员工已变得不再像以前那样忠于某一具体企业，同时也不再像以前那样对供职企业了如指掌。这种情况再加上市场的高度相互连接，为员工无意或有意干扰电子信息流动，从而造成重大破坏提供了机会。
- 随着新经济环境日渐强化，恢复旧时的传统经济运作方式已经难度越来越大，毕竟时钟不能倒转。
- 新环境经济运作的法律方面从石油和天然气工业有很多细微因素需要法律实体着重关注，转变为各部门、各公司和各国高度连接为一个整体。由于这种结构变化高速发展，法律已经显得很不适应，远远落在了当今需要的后面。

## 2. 脆弱性、后果和威胁

石油和天然气工业在持续不断地变化着。这些发展良好的基础设施由以下在物理上相互分立的物理单位组成。

- 物理基础设施：石油和天然气基础设施依靠他们的物理成分和单个独立的系统。
- 人力资源：石油和天然气基础设施依靠忠诚且勤勉的人员完成操作、维护和恢复服务等诸多方面的工作。
- 稳定的经济环境：石油和天然气基础设施在一个相对稳定的经济环境中运行。本行业的参与者、规章制度和技术始终步调一致、相互协调。

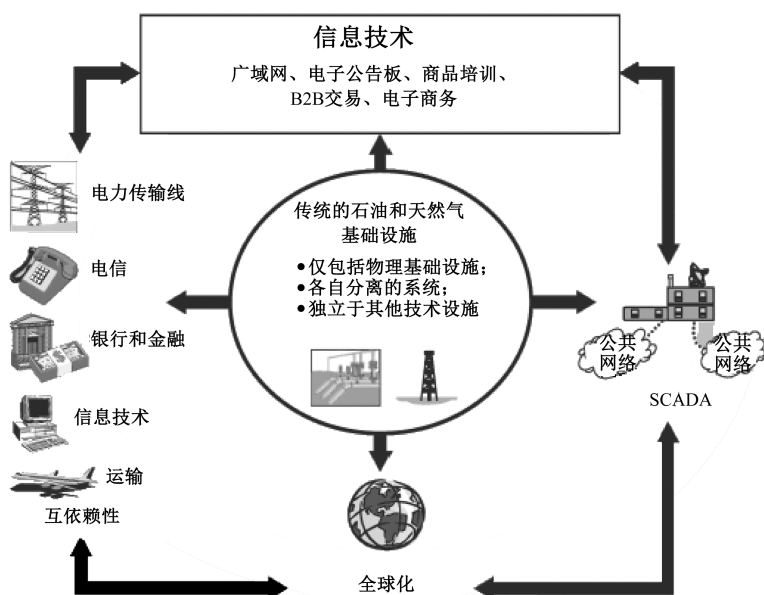
下图描绘了一个历史完整的石油和天然气行业模型。这些基础设施从世界各地获得原料，通过“制造”创造出产品，然后推向市场。此图也显示了本行业对其他基础设施的依赖。



如第 1 章所述, 信息技术和电信的快速发展和一体化使以前的系统很快过时, 创建起新的经济模式。各基础设施高度连接, 构成了一个互相依赖的复杂网络, 同时也提出了前所未有的安全挑战。当今的观点认为, 以下要素是这些基础设施赖以生存的关键。

- 信息技术和电信: 石油和天然气基础设施依赖电子商务、B2B 系统、电子公告牌、计算机网络和其他关键业务系统来进行操作和连接。
- 全球化: 石油部门已经成为跨国性行业, 这从依靠外来进口和外国公司入主美国石油天然气公司中可以窥见一斑。
- 监督控制和数据采集 (SCADA) 系统: 石油和天然气基础设施越来越依赖自动化技术操作管道系统、炼油厂和其他关键组成部分。
- 互依赖性: 石油和天然气基础设施的运行离不开电力、信息技术、电信、银行和金融、交通和供水等其他基础设施。

全球化使美国的石油和天然气工业乃至整个美国经济都变得非常脆弱。下图显示了石油和天然气基础设施的当前模型:



## 脆弱性、后果和威胁

石油和天然气工业拥有确保物理安全的成功历史。过去，即使面临自然灾害等极端事件，也能将损失降到最小。由于企业裁员、资产利用率提高以及市场的全球化发展，一整套新的脆弱性、后果和威胁通过业界对信息技术和电信的依赖而呈现在我们面前。

过去，石油和天然气工业的脆弱性和威胁大多能通过物理手段化解。我们利用大门、枪支和警卫来保卫我们的“关键资产”，而且在多数情况下效果颇佳。然而到了今天，一把“电子钥匙”便能闯过所有物理堡垒。这是一个重大转变，与新旧经济运作模式的转变如出一辙。很多潜在“网络威胁”可以毁坏或删除信息，其中包括硬件和软件故障、人为错误、居心不良的内部人员、外部黑客等。这些新威胁的后果是恢复电子登录和支持性数据时发生问题。即便是最佳物理安全状态也无法杜绝此类新型网络威胁。

信息脆弱性的存在已有好几年了。然而这些年也发生了很多变化：企业运作越来越依赖信息技术和电信，人们对这些脆弱性的了解越来越深入，并且展开了分析研究。出于本文的研究目的，我们将脆弱性、后果以及它们的相关威胁分成 7 个类别。这些分类为本部门应对当今的各种挑战提供了一个框架。具体分类如下。

- (1) 信息技术和电信：计算机、互联网和高速电信是当今商业运作的关键所在。
- (2) 全球化：互联网的问世和电信的近期进步把不断发展的世界性经济送上一列高速火车。
- (3) 业务重组：全球化、竞争和技术进步带来的变化是经济环境的重新构成。
- (4) 互依赖：石油和天然气工业不但本身互相依赖，而且还依赖电力、信息技术、电信和交通。
- (5) 政治和法规问题：政治和法规环境对石油和天然气基础设施有重大影响。
- (6) 物理和人为因素：如前面的两图所示，石油和天然气基础设施由正常运转的广阔物理网络组成。日常活动（包括人为错误）很容易造成损失。
- (7) 自然灾害：大自然的异常情况也有可能造成损失。

这 7 个类别是依据与石油和天然气行业的相关性按等级排列的。信息技术和电信与石油和天然气的关系最密切，排在第一，自然灾害排在最后。这样的排列是根据当前业界所具有的应对每类脆弱性、后果和威胁的能力确定的。虽然自然灾害是业界重点关注的问题，但是对于自然灾害，业界已经拥有一套非常成熟的处理办法，因此被排列在最后。

虽然每个类别都有自己独特的脆弱性和威胁，但是某些与后果相关的主题却是共同的。这些主题说明，如果处理不当，上述 7 个类别的任何一类都会对石油和天然气基础设施产生严重影响。每个类别都有可能以某种形式产生以下危害：

- 削弱石油和天然气基础设施的活力；
- 中断地方、地区乃至全国的石油或天然气供应；
- 破坏国家安全，摧毁美国经济。

## 信息技术和电信

如果说有哪种脆弱性，由其导致的灾难性事件会摧毁任何关键基础设施，那这种脆弱性一定是属于信息技术和电信领域的。在短短的还不到一代人的时间里，信息革命和计算机普及使商业和经济的运行发生了天翻地覆的变化。与其他基础设施一样，石油和天然气工业逐渐演变得完全依赖先进的电信和信息系统与客户、供应商联系并提供产品和服务。当今的新经济环境

是由角色越来越重要的技术以及受其影响的社会方方面面的发展塑造出来的。我们正迅速从资产经济迈向知识经济。虽然新的经济环境为石油和天然气基础设施提供了新的机遇，但同时也给保护关键基础设施带来严峻挑战。网络系统、SCADA、企业资源处理系统、自动抄表系统、基于互联网的交易、及时的后勤保障以及电子商务的不断应用使这些基础设施更加有效地运行。石油和天然气基础设施对这些技术过分依赖，而现在却还没有足够的手段来保护这些系统乃至基础设施的安全。

### 全球化

随着互联网的应用越来越广泛以及电信技术的迅猛发展，新的知识型全球经济应运而生，企业运作模式也因此而发生了根本性变化。如今已经不能再用孤立的眼光去看包括美国在内的任何经济体。全球经济给全世界的经济发展迅速带来了新的机遇。

石油和天然气工业正在与他们的供应商、客户以及其他相关经济部门一起加速迈向全球化。外国公司入主美国公司、跨国公司合并、合资企业、战略联盟以及与外国政府建立合作伙伴关系等，全都是这一过程的具体体现。

全球化对石油和天然气工业的所有者、经营者、供应商和客户产生了影响。全球化模糊了他们之间的界限，使各公司很难摸清混合型市场的变化脉络。以往，石油和天然气公司对自己的竞争对手、客户、供应商和市场了如指掌，并且有能力对它们逐一施加影响。而如今，全球化改变了这一切。

### 业务重组

随着各国迫于世界性竞争的压力寻求廉价劳动力和开放市场，当今的市场已经具有了全球化的性质。为了能在新的经济环境中生存，持续压缩成本已经成为公司必须采用的新“赌注”之一。

20 多年前，石油和天然气部门相对稳定，由一体化大跨国公司和独立公司组成。工人服务时间长，忠实于自己供职的企业，全部是经验丰富的“老手”，他们认为受家族企业雇用就是获得了一份“社会”契约。然而今天，合并、结盟和合资大大改变了公司的构成。电子信息技术的发展和交易的快捷迅速又进一步推动了这一重组过程。这种状况导致虚拟公司应运而生，企业大幅度裁员，全球性公司大量涌现，服务性公司不断改革，从而模糊了传统石油、天然气和能源公司的界限。因此，工作环境变得不再固定，以更低成本获取更高收益成为一种压力，知识和经验变成“外部资源”，“社会”雇用契约被彻底打破。

### 互依赖性

全球性的千年虫威胁充分显示了目前企业间是怎样相互依赖的。所谓相互依赖是指一种基础设施对其他基础设施的依赖。随着时间推移，由于全球化和业务重组，这样的依赖会继续发展。

### 政治和法规问题

政治和法规的不确定性使美国的石油和天然气工业很难做出长远战略决策。对基础设施的投资（即对管道、炼油厂、油井的投资）完全是根据公司的投资战略进行的。法律法规的变化因素使得很难对这些投资的回报做出估计，也很难评估某些没有投资改善其关键基础设施状况的公司可能会承担哪些责任。国家需要极具活力、能够抵御攻击并且能迅速恢复服务的基础设

施，但是这种要求与单个公司的投资战略是相抵触的。这种矛盾会极大地影响关键基础设施的保护工作。

政府常常会对某一事件造成的社会和政治压力做出反应，随之产生的立法和法规变化会对石油和天然气工业产生很大影响。为了在国家层面上推动基础设施保护工作全面展开，业界和政府必须共同找出能够让所有利益相关人接受的解决方案。

### 自然灾害

石油和天然气工业有对自然灾害威胁做出快速有效反应的能力。业界对于 Loma Prieta 和 Northridge 地震、中西部洪水和安德鲁飓风等自然灾害的反应卓有成效。在政府支持下，业界往往能够迅速联合行动起来，调集急需的设备和人员。

### 发现和结论

- 信息技术和电信发生灾难性事件或故障后会造成部分或所有关键基础设施瘫痪。
- 电信基础设施发生问题会对石油和天然气工业造成巨大影响。
- 随着石油和天然气公司越来越依赖新技术和电信系统，回归老办法的能力已经不复存在。由于公司结构发生变化，劳动力已不再像以前那样经验丰富或技能娴熟。
- 电子商务共享或公用系统的故障不但会对共享服务的成员造成负面影响，而且还有可能危及整个基础设施，从而形成一种严重脆弱性。
- 信息技术和电信系统极易被外部事件干扰。
- 流氓国家、恐怖分子或其他敌人在不断提高他们攻击网络基础设施的能力。
- 竞争压力经常导致不成熟技术投入应用，从而给企业和基础设施带来严重脆弱性。
- 石油和天然气工业依赖的信息技术和电信系统需要不断用补丁程序来弥补所用产品的安全缺陷。
- 美国能源的各种成分（即石油、天然气、电力、其他能源及其运输模式）在市场上相互融合。国家石油委员会建议，在执行第 63 号总统令的过程中，美国能源部门的各个成分应被总体视为一个能源基础设施。
- 全球化是国家经济增长的关键，但同时也给公司应对文化差异、职业道德、商业保护、法律法规、政治制度等方面的问题增加了复杂性。
- 外国公司兼并美国公司的现象给美国经济带来了新的脆弱性。
- 业界公司致力于不断提高效率和降低成本，从而导致重组、外包和裁员现象层出不穷。结果是来自不同国籍的员工、承包商、顾问、供应商形成了一个缺乏团队精神和责任感的大杂烩。
- 信息技术和电信在企业中的一体化应用造成了各基础设施之间的相互依赖。
- 基础设施间的相互依赖是关键基础设施保护工作所要涉及的一个不断发展的新方面，同时也是最难把握其给企业带来的威胁的因素之一。
- 协调一致的商业和金融法规、法律框架及国际资源的缺乏给全球化经营运作带来了严重脆弱性。
- 为了加强对关键基础设施的保护，业界与政府必须通过合作找出解决方案。
- 石油和天然气工业有能力对自然灾害和其他物理事件迅速有效做出反应。
- 石油和天然气工业拥有庞大的物理资产，其中很多资产绵延数千英里，保护工作难度

很大。

- 能源基础设施各成分的相互融合使关键基础设施保护工作难上加难。
- 依照法律规定，石油和天然气工业应该将潜在敏感信息上报政府。国会和政府部门必须确保通过相应机制防止这些敏感信息泄露给未经授权实体。

### 3. 风险管理

风险管理的重要成分包括资产评估、脆弱性和威胁分析、风险评估和降低风险方案评估。风险管理通过所有这些成分对风险做出判断并将其与其他相关因素（如成本、法律规定等）结合到一起，最终选择一种降低风险的适宜战略。

石油和天然气工业面临的脆弱性和威胁与日俱增且越来越复杂。很多公司利用风险管理的方法来应对资本投资、利率、投机和价格波动的风险。产生于信息时代的脆弱性和威胁类型以及风险性质在飞速发展变化着。因此，管理风险的关键在于制定新的预防战略和建立管理负面后果的程序。

#### 风险管理是加强关键基础设施保护的工具体

很多行业往往在重大事件迫在眉睫或发生后认识到风险存在时，才认真采用突出重点的传统方式来管理物理安全风险，这种倾向已经成为令关键基础设施系统风险消除工作大受影响的一个因素。能源部门最近出现了以更为积极的方式应对安全问题的趋势。随着网络事件造成的损失越来越大，安全也变得日趋重要。一项风险管理活动研究显示，私营部门公司的安全风险管理工作参差不齐，差异很大。石油和天然气工业在应对传统经营风险方面始终非常积极。

今天，信息技术的广泛应用带来了更多的风险。例如，用于恢复“爱虫”病毒所造成破坏的资金估计在 10 亿美元以上。不难想象，诸如此类的电子基础设施损失还会随着时间的推移而不断升级。一项行之有效的预防战略可以减少意外事件发生的次数和降低每次事件造成的损失。

很多行业都制定了协助降低风险的计划。了解风险管理战略的关键成分以及其他行业制定的相关计划，可以为在新经济环境下制定评估和降低风险的不断完善战略提供一个起始点。各个行业都因关键性事件而重新评估了自己的风险管理计划。石油和天然气工业也有一套用于传统运作的风险管理程序，而且，电子基础设施的应用以及对其的依赖表明，风险管理程序需要得到重新评估和加强。

#### 石油和天然气工业情况透视

历史上，石油和天然气工业的管理者始终对各种物理风险、通货风险、利率风险、产品责任、激烈竞争、公众信心损失、投资者信心等问题应付自如。在新经济环境下，网络风险进一步复杂化了风险管理工作。这种的复杂性部分来自越来越严重的依赖性以及为适应新经济环境而形成的高度相互连接。公司被传染了其合作伙伴和供应商的脆弱性和威胁，从而模糊了不同风险的界限。

大多数业界管理者都是从金融损失的可能性和 / 或程度的角度分析研究风险的。尽管业界管理者并不能将所有金融风险全部降低到零，但是他们能努力将风险降至某种可以接受的水平。

业界管理者通常对法律、金融和技术 / 经营风险比较关注而且经验也比较丰富，而对于意



外损失或他们本身及客户和供应商赖以生存的相互连接的电子网络遭破坏的风险，则缺乏应对能力。主要原因在于，经营风险以及为降低风险而付出的成本可以用美元来衡量，而公司基础设施的网络风险则因为涉及无形和高度不确定的潜在损失而极难估计。尽管存在这样的困难，与用于管理经营风险类似的程序亦可用来管理网络风险和其他关键基础设施风险。

可由石油和天然气工业用来管理风险的基本程序共分 6 个步骤：资产性质确定、脆弱性和威胁描述、风险评估、降低风险方案确定、降低风险行动方案选择和降低风险决策实施。这 6 个步骤在经过一定时间（如每年或每隔一年）后要重复进行，或者随风险环境的变化（如新技术问世、出现了新的威胁等）而重新报批验证。

尽管大都多风险管理计划都遵循相同的基本步骤，但是不同计划的工作力度和复杂性因行业的不同而各异。简单计划可能只需一两个关键人员在几天之内就能完成大部分步骤。而需要进行深入分析的计划则可能需要由一个分析小组用数月时间才能完成相同的步骤。就大多数情况而言，成本和时间限制是决定风险管理计划工作力度和复杂性的主要因素。通常，简单的计划就足以作为决策者提供有价值的风险管理指导。

### 确定重要资产

风险管理程序的第一步骤是确定公司的各项重要资产及其价值。这些重要资产可以是人员，也可以是设施、服务、程序或计划。接下来，要对每个重要资产的“损失影响”进行估计。这是公司资产遭到破坏或摧毁时用来计量损失的一个尺度。一种基于使用者定义标准的简单评价系统可用来计量资产的价值（分为最低级、低级、中级、高级和最高级）及其损失造成的影响。在一个更为复杂的风险管理系统中，某一资产的价值及其损失影响可用货币单位计算。这些价值所基于的参数可能包括创建该资产的最初成本、临时取代该资产的成本、永久取代该资产的成本、与收入损失相关的成本、与人员生命损失或环境资源退化相关的量化成本、与公共关系/利益相关人相关的成本以及与越来越严格的监管相关的成本。

由网络病毒和黑客攻击造成的损失尤为难以估计。据国际计算机安全协会估计，“爱虫”病毒给北美地区造成约 10 亿美元的损失。计算机安全学会 2001 年 3 月发布的报告《2000 年计算机犯罪与安全调查》证实，由计算机犯罪和其他信息安全破坏活动造成的威胁丝毫没有减弱迹象，而由此造成的金融损失则呈直线上升之势。

与新型网络经济环境相关的风险很难定义或假设，由它们带来的损失自然也很难估计。也就是说，在当前情况下，某一事件会产生超出其所在经济部门的无法预料后果。因互依赖性而出现的连锁性反应往往会超出单个公司乃至单个经济部门的控制能力。因此，要想把风险控制可在可接受的成本范围之内，各工业部门之间的协同合作至为关键。

资产的重要性决定了应该采用何种级别措施保护其免受网络或其他安全威胁困扰。有些资产，如商业机密或控制系统（SCADA），对于公司可能至关重要，乃至这种损失在经济上是无法弥补的。这些资产必须受到严格保护。传统上，预防性安全措施一直是通过隔离来实现的。在石油和天然气工业，很多公司都采用这样的战略来保护关键资产。

由于有些资产（如管理资产或文字处理软件）非常容易获得或取代，它们的保护需要十分有限。因此，只有最低程度的资源需要减少损失或降低损失风险。大多数公司资产通常都居于这两者之间。

## 确定脆弱性和威胁

风险管理程序的第二步是确定脆弱性、威胁及其特性。这个步骤涉及对各种脆弱性和威胁作周密分析。脆弱性评估可以确定弱点、验证现行资产保护措施的有效性并就应该增加哪些措施来降低风险提出建议。经常进行脆弱性评估是确保及时识别新脆弱性（尤其是与网络系统相关的脆弱性）并采取应对措施的关键。通过第三方定期评估脆弱性可以增强内部审计的客观性。

以下是脆弱性评估通常应该考虑的因素。

- 网络：
  - 网络安全——内部网络和外部网络；
  - 数据安全；
  - 系统管理——使用者或系统、桌面和服务器；
  - 检测和反应——及时采取应对措施；
  - 政策和程序；
  - 使用者的安全意识和遵守安全规章；
  - 信息系统依赖性和互依赖性；
  - 供应商、合作伙伴和供应链。
- SCADA。
- 物理：
  - 访问控制、证件管理和钥匙控制；
  - 装车平台/送货；
  - 邮政服务；
  - 障碍物、传感器、闭路电视；
  - 保安人员；
  - 社会工程；
  - 环境和安全；
  - 应急反应计划；
  - 政策和程序；
  - 使用者的安全意识和遵守安全规章。
- 提高人员安全意识计划。
- 内部和外部互依赖性。

管理风险的关键是了解资产在其中运行的威胁环境。威胁载体会通过脆弱性造成损失。威胁不断演变的性质使威胁评估成为一个动态过程。而信息源浩如烟海、政府机密情报难以获得和信息共享机制的缺乏等因素使及时收集和分析威胁信息的工作进一步复杂化了。经常性的威胁评估和及时的信息共享可以增强业界迅速应对不断变化的威胁的能力。在评估威胁的过程中，应考虑的因素包括：

- 有能力进入目标的威胁载体的存在；
- 威胁载体造成危害的能力；
- 造成危害的企图；
- 曾经表现出来的威胁载体的活动史；

- 潜在威胁载体的活动目标（过去为设施或者当今为机密信息）；
- 现有安全环境对威胁载体成功利用脆弱性的能力的影响。

威胁的程度决定于这些因素的结合程度。因素种类越多，威胁的程度越高。

典型的威胁载体包括：

- 心怀不满的员工和内部人员；
- 罪犯；
- 黑客；
- 竞争对手；
- 恶意软件；
- 自然灾害或人为错误；
- 激进分子；
- 恐怖分子。

威胁是由威胁载体的存在、能力和活动机会决定的。

威胁和脆弱性的评估需结合进行，用以估计它们给资产带来损失的可能性。尽管损失史也有助于估计可能性，但是评估与历史上并不存在的网络系统相关的威胁和脆弱性需要征求专家的判断。因此，与网络资产相比，估计物理资产损失的可能性和后果要容易得多。网络技术的快速变化、信息系统的不断发展以及网络技术和信息系统的广泛应用带来了许多脆弱性。此外，公司运作越来越依赖于及时获取信息。日趋强烈的互依赖性和高度相互连接增加了有可能给公司带来损失的脆弱性和后果。

### 风险评估

风险管理程序的第三步是根据收集来的资产、脆弱性和威胁信息进行风险评估。这一过程的目的是对每项重要资产所面临的风险做出准确估计。这个步骤涉及考虑已被确定的各种脆弱性以及综合可能性和影响信息。风险评估必须考虑的可能性因素包括：

- 有人企图利用脆弱性的可能性。尽管脆弱性是存在的，但这并不意味着就一定有人企图利用这些脆弱性。
- 利用脆弱性的企图能够成功的可能性。有些人利用脆弱性的企图会因为安全保卫措施、运气成分或自身能力的低下而失败。
- 产生一定程度影响的可能性。如果脆弱性被成功利用，会产生很多负面结果。

有各种各样的风险评估工具和技术手段可用来对风险做出估计。工具的类型取决于风险评估的可用资源和时间要求。

### 确定降低潜在风险的方案

风险管理过程的第四步是确定降低风险的方案及其特性。业界管理人员出于成本效益的考虑，往往会在众多降低风险方案中进行选择。降低风险的行动方案通常侧重于 5 个不同的方面：制止威胁载体活动、通过减少或消除脆弱性保护基础设施免受威胁困扰、通过降低风险的行动减少潜在损失事件造成的后果、通过有效的危机管理减轻事件的严重性以及快速恢复事件造成的破坏。

有些基础设施威胁载体的行为是可以通过有效的执法或国际性法律行动加以制止的。资产保护和危机管理可以通过适宜的政策和程序、技术以及机构间支持而得到加强，从而减少公司

和经济部门的脆弱性。采用降低风险的技术手段和加强机构间合作可以加快服务恢复的速度。保险可以缩小金融损失。

隔离各个资产等保护措施可以降低损失事件发生的可能性，但却不会改变影响的程度，如果资产已经损失了。有些措施既有保护成分，又有减小影响的成分。例如，防病毒软件既可以减少损失的可能性，也可以减小影响。保险等措施只适用于损失发生后的情况。降低风险措施可以减轻某事件带来的后果或提供经济补偿或其他赔偿。因此可以说，运用降低风险措施是在损失发生前、发生期间和发生后的保护资产或其金融价值的有效管理工具。

在评估降低风险方案的过程中，重要的是不仅要评估新方法，而且还要对现有的降低风险活动做出评价。在有些情况下，现行降低风险战略可能原本就成本效益很高。而在另外一些情况下，如果现行降低风险行动方案以往能够有效应对的脆弱性当前的表现程度已经大不相同，该降低风险行动方案或许已经不再需要。

各种降低风险措施的成本可以通过业界协同合作的努力降低。制定统一标准是一种既能降低成本又能确保满足合作伙伴各种不同风险管理要求的行之有效的办法。现行的 ISO/IEC 15408-1 标准就是侧重信息技术安全的标准的例子。

### **通过分析选择高成本效益降低风险行动方案**

风险管理过程的第五步是选择降低风险行动方案。企业可用于降低风险的资源十分有限。决策者必须对风险环境进行严密分析后方能确定本公司能够接受的风险水平。决策者随后需要对现有的降低风险方案进行分析研究，然后确定哪些方案适合于本公司采用。

在某些情况下，适宜的风险管理决策可能是继续实施现行降低风险方案。而在有些情况下，可能需要对现行降低风险方案进行修改或者实施新的降低风险方案。这方面工作的目的是选择成本效益最高的降低风险方案，以将风险降至某种可以接受的水平。可供决策者选择的降低风险方案越多，他们就越能将各种行动方案灵活结合到成功的风险管理计划之中。

### **实施风险管理决策**

风险管理过程的第六步即最后一步是实施风险管理决策。这是整个过程的关键性步骤。除非风险管理方案能够得到有效和高效实施，否则这种方案毫无意义。这个最后的步骤通常涉及：

- 为实施降低风险行动方案制定计划和程序。
- 为实施降低风险行动方案配置和培训人员。
- 监督降低风险的具体工作，以确保经过周密计划的方案得到贯彻执行并真正取得降低风险的效果。
- 持续主动监视威胁、脆弱性和降低风险的环境，以随时发现可能出现的变化并据此修改风险管理方案。

### **通过保险弥补损失**

石油和天然气工业的所有公司都投保了某种形式的财产险和责任险。财产险可以对投保的公司自身财产的损失进行经济补偿。责任险则可在某公司因连带对其他公司财产造成损害而必须依法赔偿对方时对该公司进行经济补偿。

各种保险都取决于确定损失货币价值的能力。就财产性机密商业信息或知识财产而言，其货币价值往往基于投资成本。例如，知识财产除非根据特许协议或合同按某种既定价格出售从

而形成市场价值，否则该财产不能为未来可能的价值投保。也就是说，公司不能为投机损失机会投保。因此，根据保险业现行规定，知识财产或其他商业敏感信息或财产信息因网络意外事件造成的损失不可投保。

业务中断险可以对公司因网络意外事件遭到的损失进行补偿，如果能够确定损失的货币价值的话。然而，由于业务的机会成本很难确定，不附带间接财产损失的业务能力的损失通常不能投保，不过损失的工作时间的价值可以投保。

目前尚无案例法是针对产生于因网络事件或其他破坏而造成的公司基础设施瘫痪的民事错误（民事侵权行为和合同履行行为）的。然而，正如本报告所阐明的那样，网络意外事件会发生的事实是可以预计的。而且，从某种程度上说，它们的发生次数是可以减少的。因此，可以预计到了将来，未能履行应尽的保护自己及其网络合作伙伴免受攻击职责的公司很可能被法律判定为玩忽职守。

某公司基础设施因网络事件而发生故障也有可能造成无法履行对石油和天然气公司按量按期供应产品的合同。在这种情况下，清算出来的损失或其他赔偿可能数额极其巨大，因此也有可能不能投保。

保险公司现在已经开始提供适用于网络风险的专项险种。购买这种保险的公司通常必须接受保险商对其进行风险评价，同时被要求实施特定的网络安全措施。

#### 发现和结论

- 对于石油和天然气工业来说，管理风险的关键是制定预防措施和对已发生事件的后果进行管理。然而，需要有新的战略和最佳实践方法来保护信息免受损失和确保关键基础设施在新经济环境下正常运转。
- 由于网络通信和计算机技术的广泛应用，同时由于利用信息技术提高企业经营效率的运作模式的采用，很多风险的界限已经模糊不清。
- 由于公司基础设施的网络风险成本涉及无形且高度不确定的潜在损失，因此很难对它们做出估计。
- 风险管理将通过采用全行业一致的网络安全管理标准而得到加强。
- 石油和天然气工业公司可从定期对自身的物理和网络系统及其运行进行脆弱性评估中获益匪浅。
- 公司需要了解或评估其合作伙伴的脆弱性。此外，公司还需了解和评估未知第三方带给其系统的脆弱性。
- 在当今高度互联的经济网络世界里，有很多风险是无法定义或假定的。因此，需要开发出能够应对这些未知风险的风险管理系统。
- 公司不能对投机损失机会投保。因此，根据现行保险业规定，知识财产或其他商业敏感或财产信息因网络意外事件而遭受的损失不能投保。
- 作为一种管理风险的工具，信息共享是石油和天然气工业加强预防和控制工作的关键因素。

## 4. 响应和恢复

响应和恢复计划与及时的威胁和脆弱性信息一起，在降低风险方面发挥着重要作用。在当

今的新经济环境下，响应和恢复计划必须考虑以下因素：

- 业界对信息技术和电信的依赖；
- 业务重组；
- 互依赖性；
- 立法和法规的不确定性；
- 自然和人为意外事件。

### 业界响应和恢复计划现状

#### （1）物理基础设施

历史上，大多数公司都懂得如何并且能够处理自己的物理基础设施遇到的问题。严谨的商业运作要求业界对由地震、飓风等自然事件以及蓄意破坏、犯罪行为、恐怖主义、意外事故等人为事件迅速做出响应。通常，这些事件会在当地造成后果。今天，越来越普遍的自动化、越来越紧密的相互连接、对时间要求越来越高的运作模式以及越来越严重的互依赖性使得发生地区性、全国性乃至国际性事件和影响的可能性越来越高。这些涉及范围越来越广的后果对行之有效的响应和恢复计划、应急响应和后果管理提出了新的挑战。

政府对安全的监管往往对企业如何制定和实施响应和恢复计划提出严格要求。例如，交通部管道安全局要求管道公司制定正规应急响应计划，并且每年都要通过演习检验这些计划的有效性。

在传统类型自然灾害方面，《斯坦福法》对联邦应急管理局（FEMA）应如何做出响应以及应如何对地方恢复工作拨款做出了规定。该法还规定了一系列标准，各州可据此申请并获得联邦资金用于本州的恢复工作。

在国际层面上，海事法对保险、海运和深海打捞做出了规定。各国还采用石油泄漏响应程序和化学物品安全法规来保护各自的环境。世界各国都在使用保险来减轻后果和为响应和恢复工作筹集必需的资金。

国际协议和国家计划可以起到预防发生严重供应中断的作用。而相互援助计划则是业界与地方政府用以对大规模事件做出响应并加以恢复的准备手段。这类计划已经存在，将不断完善具体实践方法并形成给签约各方都带来好处的网络。

石油和天然气工业的各公司之间有一些非正式协议，用以在发生突发事件时“相互借用”供应品。它们一般是口头协议，而供应品的类型涉及从管道到压缩机部件的各种物品。这些非正式协议通常建立在现场工作人员之间关系的基础上。随着人员不断流动或自动化系统取代人工操作，这种非正式协议可能会越来越少。严谨正规的相互援助协议效果更佳也更可靠。

#### （2）网络基础设施

信息和电信技术的广泛应用对响应和恢复计划提出了新的挑战。针对偶然事件的计划必须把遍布新经济环境的网络考虑进来。响应和恢复工作的复杂性和范围轻易就会超出任何单个公司应对网络危机的能力，后果涉及范围广、相互依赖、连锁反应、快速扩散、造成地区性、全国性和国际性影响是网络危机的特点。

公司如今依赖网络系统运作物理基础设施、开展电子商务和常规业务交易。因此，网络意外事件会对物理基础设施的计算机自动化控制、一体化电信系统和相互依赖的配送系统造成影响，同时还有可能造成物理破坏。此外，常规业务、交易和其他电子商务系统的事故还可以带

来巨大经济损失。事故发生的速度就像愈演愈烈的计算机病毒和拒绝服务攻击所显示的那样，对响应和恢复计划提出了新的要求。

以下是可能发生的部分网络意外事件：

- 电子交易系统损失（买方和卖方无法交易）和电子商务 / B2B系统损失（影响获得原料和服务的能力）。这两种损失都会破坏公司的正常经营。
- 未经授权改动公司交易业务。
- 关键业务系统损失或改动关键决策数据。这种损失会对公司的物理运作和经营的连续性造成影响。
- 无法使用互联网、电信或电力的损失。这种损失会破坏公司的物理运营。
- 盗窃或改动SCADA数据或SCADA系统损失。这种损失会影响运作管道或设施的能力，具有造成服务损失的可能性。
- 泄露敏感客户信息和交易信息。
- 未经授权将公司信息登录在互联网上，其中包括出于控制股价的目的散布虚假和诽谤性消息。
- 攻击和改动公司网站。
- 窃听和不正当使用敏感公司通信。

### （3）全球化、重组、政治和法规及互依赖性问题

全球化、公司重组、政策和法规的不确定性以及互依赖性问题进一步增加了制定协调一致的响应和恢复计划的难度。2000年8月19日凌晨时分，在新墨西哥州卡尔斯巴德以南20英里处发生的爆炸便是造成连锁反应的一次基础设施意外事件。这条管道是3条毗邻的天然气管道之一。亚利桑那和加利福尼亚两州的电厂依靠这些管道输送的天然气发电。管道发生破裂后，所有3条管道全部关闭，对电厂的天然气供应中断。

最初对爆炸做出响应的是地方、州政府和公司的官员。随后，管道安全局、交通部安全委员会和环境保护局也先后做出响应。事故发生地至少有6个不同单位的人员到场，他们的看法、权限和计划各不相同。最初的行动围绕着如何遏制爆炸展开，以保护周围居民以及应急响应人员的生命安全，随后则是调查管道破裂和爆炸的原因。如果怀疑这是恐怖分子所为，则还会有联邦调查局参与进来。

由于此次事件对西部地区的天然气供应有潜在影响，对管道中断供应的影响做出评估便成为工作的关键。如果天然气管道关闭的连锁反应引起以天然气为燃料的电厂供电中断，加利福尼亚会受到严重影响。交通部请求能源部提供一份能源影响评估报告。

这个事例说明了某个基础设施发生的问题会在地区乃至全国范围内产生什么影响。以下是必须考虑的问题：

- 事件的发生会超出单个公司乃至单个行业的应对能力，它的影响有可能波及其他基础设施，蔓延到很多地区乃至其他国家。
- 在对超出单个公司乃至单个行业的可能后果做出评估方面，政府应担任什么支持性角色？
- 是否应制定出应对同时发生的地震、网络攻击、能源系统瘫痪等意外事件的计划并与其他基础设施部门协同采取措施？

- 哪个政府部门有权解决司法争端并负责快速恢复服务的工作以减轻事件造成的下游后果？
- 地方和州政府（或者受影响国家的政府）应该在地区性或全国性响应和恢复工作中担任什么角色？
- 事件发生期间，哪些类型信息应该供所有相关人员共享，以从行动报告中总结出最佳实践方法或经验教训？

### 加强响应和恢复工作的最佳实践方法

#### （1）评估最佳模式

很多组织和政府机构搜集和发布有关应急响应和恢复活动经验教训的信息。例如，FEMA、EPA、交通部管道安全局、海岸警卫队、联邦调查局国家基础设施保护处和核监管委员会都是传播相关经验的联邦机构。此外，还有很多安全和紧急事件预防组织起着信息交流站的作用。将其他部门发生的意外事件的类型、频率和严重性与石油和天然气工业发生的意外事件进行比较，决定恢复服务的时间，确定阻碍迅速恢复服务的因素（如果存在的话）以及估算相关成本都是必须进行的重要工作。因此，需要加强研究工作来评估这些信息交流系统的作用，确定它们的哪些方面最适于应用到石油和天然气工业的响应和恢复计划、检验和实施工作之中。

#### （2）定期检验

当前存在着多种级别的偶然事件应对计划。这些级别都是根据具体机构及其在响应和恢复工作中扮演的角色确定的。地方政府、州政府、行业协会、联邦政府和国际组织有着不同的权限和利益取向。事件后果对它们的影响以及它们对这些影响做出的响应都必须预计并做好相应计划安排。新经济环境驱动因素的影响、全球化新兴市场以及响应和恢复的时限增加了工作的复杂性。这些越来越复杂的响应和恢复环境要求对计划定期进行检验，以确保计划能够有效管理紧急事件造成的后果和降低所有利益相关人面临的风险。公司还应根据《1900 年石油污染法》等法规定期对计划进行检验。这样的检验可以：

- 验证计划的总体适宜性；
- 验证计划的最初设想；
- 验证执行人员的能力；
- 确定未预料到的问题；
- 确定新出现的问题；
- 确定计划的缺陷；
- 锻炼人员的能力。

检验应以适宜的时间间隔进行。成熟的检验程序应该含有定时常规检验和不定时抽查检验两种形式。成功的抽查检验是公司能力的最佳指示器。随着响应和恢复计划越来越复杂，对计划做出适宜检验也难度越拉越大。单个公司可能无法检验自己应对“所有”后果的能力。在新经济环境下，可能需要多家公司结成的组织共同进行一体化检验。

#### （3）信息共享

石油和天然气工业应该建立一个正式的全行业信息共享机制，用以在意外事件发生期间向所有利益相关人传递信息。石油和天然气工业的规模和复杂性，以及就应对各种后果与其他公司、基础设施部门、地方、州和联邦政府合作的需要，要求各方在事发期间随时掌握最新信息。



信息共享机制可以：

- 在事发期间作为本部门收集和传递信息的正式中心；
- 收集用于分析的事件信息；
- 对联邦机构、州和地方政府以及事发现场指挥人员等所有利益相关人提供信息；
- 创建和维护有关关键技能、资料、服务及其他响应和恢复资源的“黄页”目录供各相关公司在事发期间共同使用；
- 提供说明和补充指导，帮助相关公司了解和解决响应和恢复计划问题；
- 发布有关响应和恢复培训和外包方案的信息以及得自政府和行业组织的其他消息；
- 向所有利益相关人提供有关部门内外响应和恢复计划最佳实践方法和标准的反馈信息。

#### 发现和结论

- 石油和天然气工业有着应对物理基础设施破坏的丰富经验。
- 石油和天然气工业依靠信息技术和电信运营物理基础设施、交易系统和常规业务程序。这种依赖性带来的后果对行之有效的响应和恢复计划提出了新的挑战。
- 用于网络意外事件的响应和恢复能力及程序不如应对物理事件的响应和恢复能力及程序成熟。业内公司需要不断审查和更新响应和恢复计划以确保它们能够解决网络方面的问题。
- 网络方面的信息是一种关键性资源，必须及时恢复。没有了信息，基础设施的恢复工作会毫无意义。网络响应和恢复计划应该建立在有效的数据备份及恢复政策和程序之上。
- 业内公司应该确保定期进行检验工作，以验证关键基础设施资产的响应和恢复计划。
- 新经济环境要求业内公司将合作伙伴、供应商、客户、地方和州政府代表等所有利益相关人都吸收到响应和恢复检验工作中来。
- 业内公司需要一个有效的内部信息共享机制，用以接收、分析和传递内部和外部资源的信息。
- 及时和具有可行性的信息是对威胁或事件做出有效响应和成功恢复服务的关键。
- 业内公司需要不断审查它们之间的相互援助协议，以确保这些协议在新经济环境下依然能够有效发挥作用。
- 在新经济环境下，网络和物理意外事件更有可能造成地区性、全国性乃至国际性连锁影响。业界应该与政府密切合作，共同制定地区性响应和恢复计划。
- 发生基础设施破坏事件时，地方、州和联邦政府的角色和责任往往是相互矛盾的。这些管辖权限的矛盾冲突会阻碍服务的及时恢复，同时还会妨碍将来的基础设施保护工作。
- 石油和天然气工业与政府之间的合作需要不断借鉴其他行业与政府合作的运作模式，以强化响应和恢复计划及事件管理的最佳实践方法。
- 为了更好地保护美国的关键基础设施，联邦政府应：
  - 明确各联邦和州政府机构（包括联邦应急管理局）的角色和责任；
  - 与业界和其他政府机构共同确定新的响应和恢复程序，相互增进对对方这方面能力的了解；
  - 帮助业界了解其与其他关键基础设施的互依赖性；

- 与所有受影响各方协调，以提供有关意外事件的准确和及时信息；
- 建立一套程序，允许临时豁免遵守限制性法规以消除关键基础设施所受影响，以此加强响应和恢复工作。

## 5. 信息共享和部门协调

石油和天然气工业早就认识到物理资产的安全必须得到保护。结果便是本行业开发出用以保护关键物理基础设施的有效手段。然而信息技术时代的到来以及随之而至的电子工具的不断涌现，要求把这样的保护扩大至电子基础设施。电子系统与物理系统和其他电子系统高度紧密连接。鉴于信息的传送速度，就有可能危害电子基础设施安全的情况尽早发出警报，这显然是对相关系统提出的要求。事实上，这种要求是根本性的。发出早期警报的有效方法之一，便是使用涉及整个行业的信息共享机制。

为了便于信息更加顺畅地在行业内流动，显然需要有一个中心点。这个中心点可以是一个人，也可以是一个机构，他或它应被指定为部门协调员，专门负责协调信息在行业内的流动。

### 信息共享

本项有关石油和天然气工业的脆弱性和所面临威胁的研究表明，本行业依赖信息技术和电信处理内部和外部事务，是极易发生灾难性事件或故障，进而对所有或部分经济部门产生巨大负面影响的方面。本项研究认为：

- 竞争的压力往往会导致采用不成熟技术，从而给企业和基础设施带来不可忽视的脆弱性。
- 石油和天然气工业需要不断通过修补来纠正硬件和软件的安全缺陷。
- 共享或公用的电子商务系统如果发生故障，不仅会对很多共享的服务产生负面影响，同时还会使整个基础设施变得十分脆弱。
- 随着石油和天然气公司越来越依赖于这些信息技术和电信系统，恢复旧时的人工方法将困难至极。由于企业结构的变化，企业员工已经不再像从前那样经验丰富或技术娴熟，况且，若没有网络工具，根本就无从操作系统，因此，重新采用旧的人工方法几乎不可能。
- 电信基础设施发生故障会对石油和天然气基础设施产生重大影响，因为局域或广域网络都是与新的经济系统紧密相连的。
- 系统对发生在外部的的事件十分脆弱，因为不再需要对系统某个具体点发起攻击或实施干扰，就能对整个系统造成破坏。
- 敌对国家、恐怖分子或其他敌人正在不断提高他们攻击我们的网络基础设施的能力。
- 信息技术和电信在企业运作中的结合使用，令各关键基础设施之间，如银行和金融、电力、供水、石油和天然气、交通、电信和信息技术，有了高度的互依赖性。

经验告诉我们，对影响信息技术系统的突发事件或新的脆弱性尽早发出警报，是保护系统的关键所在。因此，创建和积极加入石油和天然气工业的信息共享和分析中心（ISAC），是保护这一基础设施的首要任务。

石油和天然气工业已经建立了若干个信息共享论坛，至今仍在向业内企业提供各种有价值的信息。然而这些信息共享机制都是被动性的，并不能使人一目了然地看到对于保护工业基础

设施至关重要的实时信息。

石油和天然气业内公司在规模上千差万别，从全球性跨国公司到独资经营的小公司，称得上应有尽有。很多公司缺乏足够的 IT 安全员，有些小公司甚至根本没有配置安全人员。很多小公司履行着与跨国公司签署的合同，因此可以进入跨国公司的信息系统。本基础设施业内公司不能及时收到有关脆弱性的信息，当然也就谈不上及时做出响应了。以合理的成本加入信息共享和分析中心，可使本部门所有公司都能及时得到否则不可能得到的早期警报和解决方案。

石油和天然气、供水和电力等部门都离不开用来运行物理基础设施和加工程序的 SCADA 操作系统。这些系统越来越依赖开放的结构体系和互联网来发挥重要功能。而开放式系统极易被外部信息源污染，从而给整个行业造成破坏和带来巨大损失。因此，这些系统的脆弱性将因行业外的信息共享而大为缓解。

正如本报告讨论响应和恢复的第四章所述，突发事件发生期间的信息共享是确保做出恰当响应和恢复关键性服务的关键所在。石油和天然气工业的规模和脆弱性，以及通过与其他利益相关人的合作共同处理各种后果的需要，要求相关各方在突发事件发生的过程中随时掌握最新信息。

### 石油和天然气工业的信息共享要求

国家石油委员会考查了石油和天然气业内的、其他关键基础设施的以及其他行业的信息共享机制。为了使 ISAC 具有应有属性和达到期望的标准，NPC 研究了疾病控制中心等成功的信息共享模式。NPC 认为，石油和天然气部门的 ISAC 应具有以下能力：

- 最广泛接触涉及 IT 硬件和软件产品、SCADA 操作系统以及物理资产的有关威胁、脆弱性和突发事件的数据。
- 提供从全球最广泛来源（其中包括技术供应商、互联网资源、工业参与者、其他部门 ISAC、地方、州、联邦和外国政府、企业等）获得的数据。
- 能够在全局范围内实时识别、分析和传播有关威胁和脆弱性的信息。
- 以自动和人工相结合的方式大量分析数据。
- 优先处理网络突发事件，向成员及时提供警报和解决方案。
- 成员可选择匿名方式向 ISAC 报告突发事件信息。成员加入 ISAC 时也可不使用真实名称。
- 为取用威胁、脆弱性和突发事件识别信息和解决方案提供一个储存库。
- 演示运行 ISAC 的经验。
- 以成本效率极高的方式运行，确保成员的成本投入能够获取高得多的价值。

除上述要求外，国家基础设施保护中心（NIPC）还可安排石油和天然气部门指定人员之间的机密威胁信息共享。例如，在电力部门，某些业内人员拥有安全许可证，可以直接从 NIPC 接收有关威胁和脆弱性的保密信息，而这些信息在工厂是不能由一般人员共享的。这些人员随后与政府有关部门一起对信息进行筛选消密，以某种实用格式交由业界普通人员共享。

### 信息共享的问题和挑战

对于石油和天然气工业来说，信息共享称得上是一个杠杆支点，可加强业界人士对业内公司、整个行业、其他行业以及政府部门的了解。信息共享可以帮助提高业界人士对脆弱性和威胁的认识，进而改进响应和恢复计划，化解风险。然而，要想最大程度地发挥信息共享的作用，

还必须消除阻挠信息共享顺利进行的障碍。这些障碍便是与行业内共享信息、行业与政府共享信息以及政府与行业共享信息有关的问题。以下各节将对这些问题逐一进行讨论。

#### （1）业内共享信息的问题和挑战

如前文所述，石油和天然气业内现在已有信息共享机制在运行。信息共享存在于业内公司、贸易协会和研究机构之间。然而，有很多挑战阻碍了某些必要信息的共享。要想使信息共享有效实施，就必须正视这些挑战。这些挑战包括：

- 石油和天然气工业的规模和复杂性；
- 加入 ISAC 所带来的责任；
- 反托拉斯法和信息共享。

#### （2）业界与政府信息共享的问题和挑战

虽然业内的很多信息都可以与政府部门共享，但是眼下有几个障碍阻止了信息共享的深入展开。要想有效实施信息共享，就必须清除这些障碍。关键基础设施的保护永远离不开私营部门与公共部门的密切合作。这种合作关系的有效建立，取决于信息共享障碍问题的解决。这些障碍包括：

- 公司敏感信息的保护；
- 州和地方政府的角色；
- “千年虫”防范和责任法。

#### （3）政府与业界信息共享的问题和挑战

联邦政府在与石油和天然气工业的信息共享中扮演着重要角色。联邦政府提供实践方法和情报方面的信息，可帮助业内公司深入了解它们所面临的风险并引导它们进一步认识可选用什么适宜手段来消除脆弱性和化解风险。

目前有很多障碍阻挠了政府对业界信息共享的深入展开。政府在这方面面临的最大困难，是如何对业界共享政府从业内收集的保密和非保密情报信息和威胁信息。政府对业界共享信息的障碍包括：

- 信息共享保密的影响；
- 与外国公司分支机构信息共享所受到的影响。

#### （4）关于信息共享的建议

国家石油委员会建议开发和创建一个石油和天然气 ISAC。这样的 ISAC 有助于消除本部门依赖 IT、电信和 SCADA 操作系统的综合风险。此外，由于石油、天然气和电力构成了能源工业，对于这些行业已经不能单独进行分析。大多数能源公司都经营着两种或两种以上能源商品。NPC 建议，石油和天然气行业 ISAC 开始运行后，应考虑把其他有明显相互关联的实体业吸收进来。

尽管某些类型的信息的共享还存在问题和挑战，但是这并不妨碍 ISAC 的发展。在眼下的障碍被去除之前，很多信息还无法与政府共享。然而随着更多的障碍被扫清，ISAC 的价值会进一步体现。

NPC 建议，应与政府初步做出安排，批准部分业内人员获得国家安全许可证，使他们得以接触有关威胁的机密信息，从而加强本部门的脆弱性评价工作。

为了在不受反托拉斯法干扰的条件下推动信息共享，NPC 建议 ISAC 向司法部申请业务运作批准书，以利于有关网络安全的信息共享。

NPC 认为，面向业界的服务供应商模式是最适合石油和天然气部门的最有效模式。本章前文所述的 ISAC “信息共享要求” 应被用作挑选最佳服务供应商的依据。信息技术的电信脆弱性应是工作的重点，但是随着 ISAC 的发展，还应把物理脆弱性和威胁信息也包括进来。国家石油委员会发现，有些能源公司得不到足够的这类关键信息，有的甚至连一点信息都得不到。此外，有的公司根本就没有安排物理或 IT 安全员来处理这类关键信息。成本效益出色的 ISAC 应允许这些公司接触有关脆弱性和威胁的实时信息及解决方案。

关于 ISAC 结构和操作程序，NPC 建议建立一个行业委员会来进行本部门 ISAC 的调研、开发和创建工作。这个委员会应负责解决成员资格、法律结构、成本、选择服务供应商等问题。

### 部门协调

#### （1）目的

国家石油委员会是一个联邦顾问委员会，应能源部长的要求就石油和天然气及所属行业的问题提供忠告、信息和建议。因此，NPC 接受临时担任部门协调员的角色，领导石油和天然气部门响应第 63 号总统令开展相关工作。能源部长在要求信中指出：“我希望委员会在报告的结论中，就部门协调员这一永久性角色以及如何确定哪个人或哪个机构担任这个角色提出建议。”

#### （2）讨论

有关部门协调员角色和责任的信息已在政府发布的有关关键基础设施保护的几份文件中有所描述。这些文件包括“总统关键基础设施保护委员会”和有关“第 63 号总统令的非机密白皮书”。第 63 号总统令所列各部门的目标包括：

- 评价本部门面对网络或物理攻击的脆弱性。
- 提出消除严重脆弱性的计划。
- 开发识别和预防重大攻击企图的系统。
- 制定警报、遏制和挫败攻击的计划；与 FEMA 适度协调，在攻击后快速恢复最低基本能力。
- 确保所有计划和行动均考虑了州和地方政府以及第一响应者的需要、活动和责任。
- 大力鼓励创建私营部门 ISAC。

安排部门协调需要考虑三大问题：被指定的组织或个人实施领导和与各利益相关人日常交往的能力、与行政官员的接触以及支持部门活动的资金提供。

对若干现任部门协调员的调研表明，每个部门都采用了不同方式应总统令的要求和根据业内成员的情况来实现关键基础设施保护的目标。每个部门协调员都在以不同方式履行实施领导、配置人员和提供资金的职责。因此，现在应该是石油和天然气工业决定以什么最佳方式提供这种重要领导和协调功能的时候了。

#### （3）有关部门协调的建议

国家石油委员会确定了适合于石油和天然气工业的部门协调员的角色和责任：

- 领导石油和天然气部门的关键基础设施保护事务（如推动建立本部门 ISAC 和参与 ISAC 的管理等）。
- 在本部门的关键基础设施保护事务方面充当与业界、能源部、其他关键基础设施保护部门、政府的行政和立法分支、媒体以及州和地方政府部门进行沟通的主要联系人。
- 确定部门协调员机构运行的财务结构。

- 从本部门挑选人员组成工作组，负责满足培训需要、实施提高人员认识方案、确定部门研发需要等关键基础设施保护问题和行业目标。
- 鼓励业内各部门就信息和电信系统及物理安全定期进行风险量化评价，以提高对新脆弱性的认识。

## 发现和结论

### (1) 信息共享

- 经验告诉我们，对突发事件或影响信息技术系统的新脆弱性早期发出警报对于系统保护来说至关重要。
- 石油和天然气业内有若干个共享信息论坛，但是没有指定涉及关键基础设施保护网络方面的信息共享机制。
- 通过 ISAC 进行信息共享被证明是消除和化解网络脆弱性和威胁的一种极具价值的方式。
- 石油和天然气工业将因 ISAC 的建立而大受裨益。NPC 认为，在关键基础设施常用的 3 种模式中，面向业界的服务供应商最适合运营石油和天然气工业的 ISAC。
- 业界对信息技术和电信的依赖带来了不可忽视的脆弱性。因此 NPC 建议 ISAC 的初期工作重点应该放在信息技术和电信上。
- 本部门的很多公司没有数量足够的 IT 安全员支持其系统，规模较小的公司甚至根本没有配置 IT 安全员。加入 ISAC 可为这些公司提供一种具有高成本效益的方法，用以及时获取有关网络安全突发事件和解决方案的数据。
- 业界接触有关威胁的机密信息，可进一步加强石油和天然气基础设施的保护工作。业界应与政府部门做出安排，初步允许部分业内人员获得国家安全许可证，以使他们得以接触相关保密信息。
- 石油、天然气和电力工业在市场上是融合在一起的，业内公司通常经营两种或两种以上能源商品。在接下来的工作中，应该考虑为能源业所有公司提供机会加入石油和天然气工业 ISAC。
- 石油和天然气、电力及供水工业都采用了 SCADA 操作系统。因此，将来应该考虑吸收私营供水公司加入石油和天然气工业 ISAC。
- 结构适宜的工业信息共享机制可在现行法律下运行。
- 石油和天然气业对政府的反托拉斯态度十分敏感。应向司法部申请涉及反托拉斯法的业务运作批准书。比较好的长期解决方案应该是通过新的立法。
- 要想推动业界对政府的信息共享，需要在立法方面有所行动，以解除《信息自由法》规定的相关责任。
- NPC 确定了用以促进石油天然气业内信息共享的 ISAC 要求和选择标准，这些要求和标准是选择服务供应商的依据。
- 石油和天然气工业 ISAC 的管理机构应平衡配置来自本行业各个部门的代表。

### (2) 部门协调

- 部门协调是实施有效的关键基础设施保护计划的重要组成部分，通过这种协调，可确保对日常处理基础设施保护问题的全面领导，同时又能确保各方的顺畅沟通。

- 目前尚无一个机构可代表石油和天然气工业的所有部门。本行业 ISAC 的管理机构应该是为业内协调问题提供中性论坛的理想实体。
- NPC 建议，应由能源部长正式认可石油和天然气工业 ISAC 的管理机构担任部门协调员，由他来履行第 63 号总统令提出的各项职责。

## 6. 有关信息共享的法律法规问题

众所周知，现行法律法规系统会对采取或禁止行动的决定产生影响。同样显而易见的是，为某一目的制定的某些法律法规会产生与该目的完全无关的突发后果。任何为确保关键基础设施安全而做出的全国性或国际性努力，全都必须考虑现行法律法规会对这些努力起推动还是抑制作用。本章将讨论会对石油和天然气工业关键基础设施保护的共同努力（信息共享）产生影响的相关法律法规。

为了达到分析现行法律的目的，首先需要确定这样几个条件：（1）自愿而非强制性地公开有关确保基础设施安全的信息是相关各方所期望的；（2）在什么信息应公开、应向什么对象公开以及应在什么时候公开的问题上，各方存在一致意见或者各方能够达成一致；（3）自愿公开信息的商业或政治障碍是可以消除的；（4）当前存在或者行将开发出能够确保所公开的信息的安全的技术。

由于现行法律法规有可能阻碍业界的自愿参与，确定应该怎样修改法律法规才能使业界参与信息共享的方案发挥最大效用，就显得至关重要了。本章将对现有的法律法规问题进行讨论，同时提出一些修改法律和调整程序的建议，以帮助私营部门交流共同的脆弱性、威胁、解决方案、最佳实践方法、安全遭破坏及补救措施等方面的信息。

### 信息公开和信息共享的法律障碍

如本报告前文所述，关键基础设施保护信息共享方案的任何私营部门参与者在信息共享方面都要面对两种不同的法律障碍：产生于信息将仅仅在参与者所处行业内共享时的障碍，以及产生于信息将扩大范围、与政府机构或实体共享时的障碍。总体而言，业内公司在某一特定行业内的信息共享主要牵涉是否违反反托拉斯法的问题，其中包括对机密信息的保护以及由于终止合同或违反州侵权行为法而所可能带来的责任。与联邦政府的信息共享不仅会造成同样的问题，同时还会因此而导致对提供给政府的信息应以何种方式传播或使用的失控。然而通过正视信息共享的这些法律障碍，同时制定出消除或减少障碍的政策，是完全有可能最大程度地解决这些问题的。下面，我们将具体论述私营-公共部门信息共享的法律障碍以及应如何化解由此带来的风险。

### 有关部门内信息共享的法律问题

任何旨在推动业内参与者间合作的计划都必须考虑某些法律会对行业内的信息共享产生什么影响。首先必须确定，所提出的业内信息共享计划是否具有合法性，其未来的参与者是否有能力承担组织和运行这种合作计划的责任。

应该指出的是，这些问题与计划对参与者提出的作为加入条件的义务有关。例如，其中包括参与者将负有公开信息和信息共享的责任，以及不履行这种责任的法律后果。这些问题至关

重要，在任何信息共享计划的加入协议中都应特别强调。不过下文将概括性阐明有关私营部门内公开信息的计划会给参与者带来哪些风险。

- 业内信息共享和反托拉斯法：从操作的性质上说，信息交流从来还不曾引起过反托拉斯法的严重问题。然而，随着所需交流的信息范围的扩大，业内公司将需要当心与竞争对手交流信息所带来的反托拉斯法风险，因为通过这些信息，极有可能探明竞争对手的情况和计划。
- 信息收集/共享和隐私权：公司做出严密监视其计算机网络（其中包括严密监视其计算机网络进入者的活动）的决定，极有可能令自己承担责任。例如，如果某公司确定某个访问其网站的人在访问期间试图穿过防火墙，它将这一信息通报给参与其关键基础设施保护计划的其他公司，其中包括该访问者在访问网站时有意或无意留下的任何个人信息，这种行动就会因为以下事实而令该公司承担责任：根据某些法律条款，公开某人的私人情况（即便这些情况属实）通常属于违法侵权行为，任何理智的人都会反对这样公开自己的情况。跨国公司也必须注意其运营所在国的隐私权法。在美国，向某个 ISAC 公开信息可能会危害公众利益，而公开威胁关键基础设施的信息可以认为也属于此列。《宪法第一修正案》和其他保护性法律可能适用于防止承担由信息收集活动带来的责任。
- 信息使用和诽谤：信息共享机构的成员很有可能遭到诽谤指控，这种前景似乎有些遥不可及，但是对于这样的可能性，做一番讨论还是必要的。根据普通法，诽谤是指向第三者公开会损害某特定对象声誉的信息。这个涉及面相当广的定义近些年来已被最高法院逐渐缩小了范围。最高法院一直在寻求让《宪法第一修正案》在保证言论自由和新闻自由方面发挥更大作用。然而，如果某信息共享机构的成员公开会对某个人、某家公司或某家公司的产品造成伤害的信息，而事后证明该信息并不真实，那么这个成员依然有可能受到诽谤指控。如果信息被泄露方能够拿出证据表明自己确实受到伤害，则该成员（或许会是整个机构）要承担由此产生的法律责任。
- 公开特许或机密信息：会有越来越多的私营机构公开各种类型信息，这样的前景引起了一种多少有些偏离主题的担忧：由任何公开信息行为带来的特许权很可能因此而被自动放弃。在公司上层和公司律师指导下公开否则会得到特许的信息，可能意味着就该信息本身和相关同类问题的信息自动放弃特许权。根据现行法律，就某一特定问题公开任何特许交流信息，就意味着自动放弃就同类问题进行任何交流的特权。因此，如果事先没有在信息共享机构内相关各方之间或者在该机构与联邦政府之间达成共识，说明特许权不会因为出于基础设施安全的目的而被自动放弃，相关方面通常是不愿意自愿公开这类信息的。
- 不公开或不使用信息：申请加入某项信息共享计划的业界参与者还可能会在面对因不公开或不使用有关关键基础设施遭受攻击的信息而必须承担法律责任的可能性时望而却步。从理论上说，前一种法律责任是指信息共享机构的成员有义务（这是不可选择的）与机构其他成员共享有关攻击的信息。然而，如果成员协议中对这种义务没有明确规定，要想得到联邦或州法律的保护也就无从谈起。



### 有关业界与政府信息共享的法律问题

旨在保护国家关键基础设施的合作和协调系统会因政府（包括联邦政府和州政府）的参与而得到加强。政府有权接触私营部门不对外公开的数据和情报，可以在抵御网络攻击的工作中发挥极具价值的作用。然而，双方都应提供和获取信息的政府介入会在业界潜在参与者中引起对隐私权、法律责任和安全的担忧。对于这些担忧和现行法律制度，必须进行认真考虑，政府和私营部门之间旨在确保国家关键基础设施安全的任何合作，都必须将其与最终目标做权衡比较。

- 《信息自由法》（5 U.S.C.522）：《信息自由法》（FOIA）允许“任何人”寻求进入不属于 9 种豁免权或 3 种执法特例之列的任何政府“机构记录”。如果在未来的基础设施保护方案中政府要求自愿公开信息，那就应密切注意在向某政府部门公开敏感商业信息时这些豁免权是否足以保证这些信息免于对公众公开。
- 《隐私权法》（5 U.S.C.552a）：《隐私权法》规定，有关美国公民和永久定居者的保存在某一“记录系统”中的任何个人信息，除非属于若干种特例之一的，否则不得公开。这样的豁免权允许任何政府部门负责人规定某“记录系统”免于公开，即便该系统包含了执法功能，记录内容可供司法调查之用也是如此。
- 商业机密保护：业内公司还有一种与信息共享相关的担心，那就是它们有可能丧失对商业机密（或其他财产信息）的保护。保护商业机密可以给很多公司带来优势地位，因为商业机密有可能给公司带来永久性保护，而且维持商业机密不需花费专利成本（同时也不必向公众公开发明的细节）。此外，所谓商业机密，并不一定就是重要的先见之明信息，它可能是不为常人所知、可以给其所有者带来商业竞争优势的任何信息、设计、装置、工艺、作品、技术或配方。由于有关商业保护的基本要求之一，是受保护的事物不为常人所知，因此，自愿向政府公开的商业机密信息可能会被有意或无意泄露给公众，从而使商业机密失去保护，这种风险是阻碍私营部门参与者自愿向政府公开商业机密信息的主要问题所在。
- 阳光法：州或联邦政府为推动信息共享而付出的任何努力，都必须考虑要求政府公开某些工作进程的“阳光法”所普遍存在的自相矛盾性。一方面，各州普遍规定有关公共安全的事务免受阳光法制约；另一方面，在各州的阳光法及法院实施之间存在着相当大的差异。就执法而言，各州为在个人隐私权和公众接触信息之间形成某种平衡而付出的努力，造成了各种各样的阳光法豁免，从而只能对政府当局和请求获取信息者提供指导。此外，有些州模仿联邦 FOIA 把豁免阳光法的情况划分为多个级别，另一些州则依赖本州立法者制定法规的能力。

上述问题迫使准备实施信息共享计划的行业认真考虑邀请政府在计划中担任角色有什么利弊。对这样的情况没有正确答案可言，因为相关行业做出的决定完全取决于该行业接受某种交易的意愿，接受这种交易便是对得到政府帮助和信息的回报。就依旧基于私营性质的合作关系而言，有一种类似的公共-私营部门合作安排也能发挥同样的作用。后一种安排的不同点在于，它们的基础是明确了所涉各方的角色和作用的协议。其中最重要的协议是与相关政府机构签订的有关适当使用和/或公开因参与计划而获得的信息的“谅解备忘录”。就加入协议而言，

它也可以依照向政府报告有关攻击的信息的责任吸收私营部门参与者。谅解备忘录尽管不那么容易通过谈判达成，然而对于旨在让公共部门和私营部门在关键基础设施保护上携手合作的任何安排来说，它却是至关重要的。

### 独立向政府公开信息

如果业内公司与政府之间不能就信息共享达成双方均可接受的条款，那么公司仍有可能选择就关键基础设施的某些脆弱性问题独立向政府汇报的方式。与前文所述对公开信息形成阻碍的情况恰成对照的是，这种确保与政府之间相互信任的顺畅交流信息的方式，是通过保密说明函或信息不公开协议实现的。这样的协议已经被私营部门和政府机构广泛采用。

在确保基础设施安全的背景下保证信息不公开和保密会带来一系列复杂的潜在问题，其中包括：向政府公开的信息是否可以进一步公开？公开信息的公司是否有义务有意或无意进一步公开信息？唯有这些问题得到解决之后，业界参与者才能放宽心地依靠信息共享机制。

在实施任何包含了这类协议的基础设施安全保障模式之前，需要把这样的问题一一解决。

### 鼓励信息共享的立法提案

上届国会会议提出了若干提案，它们将有助于消除或减轻业界对与政府共享关键基础设施信息的担心，可能新带来的出于网络安全目的免除《信息自由法》责任尤为引人注目。《网络安全信息法》（H.R.4246，第106届国会，2000年4月12日）便是其中之一。这项立法提案鼓励信息安全公开，保护与基础设施安全相关的信息交流。提案旨在免除《信息自由法》对网络安全数据的制约，防止数据向第三方泄露，同时豁免数据“被任何第三方直接或间接用于遵照任何联邦或州法律而进行的任何民事活动”。该法还包含了一项信息交流的反托拉斯法豁免权，目的是推动或“帮助矫正或避免网络安全问题造成的影响”。然而，该法把网络安全数据“被用来涉及或形成某项联合抵制任何人、瓜分某个市场或者规定价格或产量的协议时的情况”列为上述豁免权的例外。至于这个豁免权例外是否会导致某些信息的合法公开降温的问题，目前还没有人考虑。法案将授权总统组建联邦雇员工作组参与业界信息共享机构的工作，帮助实现该法提出的目标。

如果《网络安全信息法》提案得到通过，它将成为保护其他有益的信息交流的一种模式，可用以支持基础设施保护工作免受潜在法律后果的困扰。预计到第107届国会会议上，还会有类似的立法法案被重新提出。对于为关键基础设施保护而寻求在公共部门和私营部门之间建立合作关系的业界参与者来说，应密切关注这些立法提案的动向。

### 发现和结论

- 向司法部申请获得业务运作批准书能够最大程度地化解信息共享的反托拉斯法法律责任风险。
- 应建立一个 ISAC，以确保信息共享不会侵犯隐私权。
- 在必要的时候，业内公司应忠实无误地传送有关对本行业关键基础设施安全构成了威胁的对某一特定产品或个人不利的信息。
- 在 ISAC 的创建和运作过程中，大部分潜在法律责任都可以通过签署 ISAC 成员协议、

ISAC 服务供应商协议和制定 ISAC 成员规则等若干种合同安排有效分摊风险而得到最大程度的减少。

- 与政府的信息共享可能会导致在《信息自由法》制约下信息被泄露给第三方。但是，通过签署内容得当的正式谅解备忘录或其他类似的协议，与政府实现信息共享还是可行的。
- 其他部门的信息共享机制，如金融服务 ISAC，目前已在运行之中，它们成功处理了法律和责任的问题。

## 7. 研究与开发需要

支持关键基础设施保护的研发目标，是开发出技术和程序，用以消除脆弱性和抵御对影响着国家安全、经济健康和社会稳定的领域的威胁。石油和天然气工业主要依靠商业供应商从事信息技术、电信和监控和数据采集（SCADA）操作系统方面的研究与开发工作。因此，石油和天然气工业几乎不具备进行研发的核心力量。

政府资助的研发项目侧重于国家安全和关键基础设施保护等重要问题，而这些问题的解决超出了石油和天然气业内公司的能力范围。政府应该与业界携手合作，着重和优先实施与业界直接相关的研发项目，确保研发成果能够迅速应用到关键基础设施保护工作中。

1996 年，总统关键基础设施保护委员会确定了若干个涵盖了所有关键基础设施的研发主题：

- 保护基础设施；
- 检测入侵；
- 消除破坏的影响；
- 加快恢复；
- 开发分析或支持性技术。

政府所面临的挑战，是如何与石油和天然气工业以及其他关键基础设施行业合作，帮助重点开展研发，挖掘现有技术的潜力和加强对基础设施的保护。在这种合作中，将政府资助的研发成果转让给业界投入使用，是一个重要环节。

### 提议的研发需要

本节讨论的研发是从石油和天然气工业的角度提出的，从具体的信息技术、电信和互依赖性到物理资产保护，涉及范围很广。其中大部分需要对于其他基础设施行业也同样具有价值：

- 信息安全保障；
- 互依赖性和系统复杂性；
- 物理保护评价；
- 多传感器和警报系统；
- 保护系统和消除影响；
- 风险管理；
- 关键性后果分析；

- 加强 SCADA 保护；
- 监视和检测；
- 模化和模拟；
- 决策支持；
- 机构障碍。

#### 发现和结论

- 石油和天然气工业主要依靠商业供应商开展信息技术、电信、电子商务、SCADA 操作系统以及关键基础设施保护相关方面的研发工作。
- 政府资助的研究侧重于那些其问题的解决超出了行业能力范围并且涉及国家安全的领域。这些研究成果的投入使用可帮助业界加强对关键基础设施的保护。这方面的努力需要基础设施所有者和运行者与政府及其研究机构的密切合作。
- 政府将独自面对的一个挑战是制定出技术转让计划，以加速基础设施保护手段在石油和天然气工业以及私营部门其他关键基础设施的投入使用。

---

## 十九、第 7 号国土安全总统令：关键基础设施标识、优先级和保护

美国白宫

2003 年 12 月 17 日

---

## 1. 目的

本总统令确立了联邦各部局用来标识美国的关键基础设施和重要资源，并对其进行优先级排序和保护，防止恐怖分子袭击的国家政策。

## 2. 背景

恐怖分子试图破坏美国境内的关键基础设施和重要资源，试图使它们失去作用或遭到毁坏，从而引起大规模灾难，削弱我们的经济，并打击公众士气和信念。

美国是一种开放的、技术化的复杂社会，包括了大量关键基础设施和重要资源，它们有可能成为恐怖分子的目标。大部分这些关键基础设施和重要资源被私营部门以及州或地方政府所拥有和运行，它们既有物理形态，也基于信息技术，并横跨了所有的经济部门。

关键基础设施和重要资源提供了基础性的服务，是美国社会的支撑。国家拥有大量的重要资源，一旦被恐怖分子破坏，便有可能对人民健康带来堪比大规模破坏性武器的巨大影响或伤亡事件，或者深刻影响到我们国家的荣誉和士气。此外，有些关键基础设施事关重大，在恐怖分子袭击中一旦失去作用或遭到破坏，将会对安全和经济利益造成削弱性影响。

虽然不可能保护全国所有的关键基础设施和重要资源，也不能消除其中全部的脆弱性，但对安全做出战略性的改进后，是能够给恐怖分子袭击带来难度，并削弱袭击可能引发的后果的。除战略性的安全增强外，还可以迅速实施战术性的安全改进，遏止、缓解或减弱可能的袭击。

## 3. 定义

在本令中：

(1) 术语“关键基础设施”与 2001 年美国《爱国者法》第 1016 (e) 款（《美国法典》第 42 编第 5195c (e) 款）中的术语一致。

(2) 术语“重要资源”与 2002 年《国土安全法》第 2 (9) 款（《美国法典》第 6 编第 101 (9) 款）中的术语一致。

(3) 术语“部”指国土安全部。

(4) 术语“联邦部局”指《美国法典》第 5 编第 101 款列举的行政各部及国土安全部、《美国法典》第 5 编第 104 (1) 款定义的独立机构、《美国法典》第 5 编第 103 (1) 款定义的政府企业以及美国邮政管理局。

(5) 当用于地理意义时，术语“州”和“地方政府”与 2002 年《国土安全法》第 2 款（《美国法典》第 6 编第 101 款）中的术语一致。

(6) 术语“部长”指国土安全部长。

(7) 术语“（基础设施部门）特定机构”指负责指定的关键基础设施部门或重要资源部门的基础设施保护活动的联邦部局。在本令中，特定于各部门机构将根据部长提出的指南展开工作。

(8) 术语“保护”和“安全”指减少关键基础设施或重要资源的脆弱性，以遏止、缓解或

减弱恐怖分子袭击。

#### 4. 政策

美国的政策是加强对我国关键基础设施和重要资源的保护，防止有可能造成如下后果的恐怖行为：

- (1) 给人民健康带来堪比大规模破坏性武器的巨大影响或伤亡事件。
- (2) 削弱联邦各部局履行其重要使命、确保公众的健康和安全的能力。
- (3) 损害州和地方政府维护治安并实现基本的重要公众服务的能力。
- (4) 破坏私营部门有序发展经济功能、提供重要服务的能力。
- (5) 对其他的关键基础设施和重要资源造成灾难性破坏，从而产生负面经济影响。
- (6) 削弱公众的士气及公众对我们国家的经济和政治制度的信任。

联邦各部局将标识关键基础设施和关键资源，并对其进行优先级排序，协调保护工作，以预防、遏止和降低那些试图破坏这些关键基础设施和重要资源的恶意行为所带来的影响。联邦各部局将与州和地方政府以及私营部门相合作，共同实现这一目标。

联邦各部局将确保国土安全诸计划不会对美国的整体经济安全造成不利影响。

在实施本令时，联邦各部局将认真保护有关信息，包括依据 2002 年《国土安全法》以及其他可适用的法律来处理自愿提供的信息以及有可能被恐怖分子所利用的信息。

联邦各部局在实施本令时应与相关法律中的条款保持一致，包括美国人身权保护法律。

#### 5. 部长的角色与责任

在落实 2002 年《国土安全法》中要求的职能时，部长应该负责协调整个国家的关键基础设施和重要资源的保护工作。部长应作为首席联邦官员来领导、整合并协调联邦各部局、州和地方政府、私营部门之间的关键基础设施和重要资源的保护工作。

根据本令，部长将负责标识关键基础设施和重要资源，并为之排列优先级，协调对关键基础设施和重要资源的保护。重点在于那些一旦被破坏便有可能对人民健康带来堪比大规模破坏性武器的巨大影响或伤亡事件的关键基础设施和重要资源。

部长将确立统一的政策、手段、指南和方法，整合联邦政府在各个部门之内以及各部门之间的基础设施保护和风险管理活动，相关的计划和活动要有衡量准则和标准。

部长应该协调下述每个关键基础设施部门的保护工作：信息技术、电信、化学、运输系统（包括大型客运、航空、海运、货运/地面运输、铁路、管道系统）、应急服务、邮政和船运。国土安全部将同有关的部局相协调，确保其他重要资源得到保护，包括大坝、政府设施和商业设施。此外，国土安全部作为总的跨部门协调员，还应在以后必要时评估是否需要保护并协调其他的关键基础设施和重要资源的安全工作。

部长将始终运行一个作为 cyber 安全工作焦点的机构，该机构将推动联邦各部局、州和地方政府、私营部门、学术组织以及国际组织之间的交流与合作。在法律许可的范围内，拥有信息技术专家的联邦各部局，包括但不限于司法部、商务部、财政部、国防部、能源部、国务院和中央情报局，将与国土安全部内的这一 cyber 安全机构合作，支持其完成使命。该机构的使

命包括分析、预警、信息共享、脆弱性削减以及援助国家对关键基础设施的信息系统进行的恢复工作。在法律许可的范围内，该机构将支持司法部及其他执法机构对网络空间威胁和攻击实施的调查及诉讼。

在实现本令目标的过程中，部长将与联邦各部局、州和地方政府以及私营部门密切合作。

## 6. 对口联邦机构的角色与责任

认识到每个基础设施部门都有其独有的特征和运行模式，因此指定了如下（基础设施部门）特定机构：

- （1）农业部——农业、食品（肉、禽、蛋产品）；
- （2）健康和公众服务部——公共卫生、保健和食品（除肉、禽、蛋产品之外的其他食品）；
- （3）环境保护局——饮用水和水处理系统；
- （4）能源部——能源，包括石油和天然气、电力产品的净化、存储和配送（商业原子能设备除外）；
- （5）财政部——银行和金融；
- （6）内政部——国家纪念物和圣像；
- （7）国防部——国防工业基地。

依照部长提供的指南，各个特定机构将：

- （1）与所有相关的联邦部局、州和地方政府以及私营部门合作，包括基础设施部门中的关键人员与实体；
- （2）实施或推动对基础设施部门的脆弱性的评估；
- （3）鼓励实施风险管理战略，以保护关键基础设施和重要资源，减缓关键基础设施和重要资源遭到攻击后带来的影响。

本令不会改变或阻碍联邦各部局根据法律、可适用的法律文件以及总统指令而行使其职责的能力和权力。

联邦各部局应与国土安全部合作执行本令，并保持与 2002 年《国土安全法》及其他可适用的法律文件一致。

## 7. 其他部、局和办公室的角色与责任

除了赋予国土安全部和特定联邦机构的责任外，关系到关键基础设施和重要资源保护的各联邦部局以及各个总统行政办公室有下述特殊职能：

- （1）在与国土安全部、司法部、商务部、国防部、财政部及其他有关联邦机构的联合下，国务院将与外国政府以及国际组织合作，加强对美国的关键基础设施和重要资源的保护。
- （2）司法部（包括联邦调查局）将负责减缓国内的恐怖分子威胁、调查和起诉实际或酝酿中的恐怖分子对关键基础设施和重要资源的袭击和破坏。司法部长和国土安全部长应利用可适用的法定权力及伴随机制来实现合作和协调，包括但不限于总统令确立的权力和机制。
- （3）在国土安全部的协调下，商务部将与私营部门、研究组织、学术组织和政府组织相合作，以改进信息系统技术，推动其他的关键基础设施工作，包括在《国防生产法》的授权下确



保工业产品、材料和服务的及时可用，以满足国土安全的需求。

(4) 关键基础设施保护政策协调委员会将就物理和信息基础设施保护方面的跨机构政策向国土安全委员会提出咨询建议。协调委员会的主席将由一位联邦官员或由国土安全总统助理任命的人员担任。

(5) 在国土安全部的协调下，国家科技政策办公室将协调跨机构的研究和开发工作，以增强对关键基础设施和重要资源的保护。

(6) 管理和预算办公室（OMB）将监督与联邦政府计算机安全项目有关的政府层政策、原则、标准和指南的执行。OMB 主任将确保运行一个中央的联邦信息安全事件中心，与 2002 年《联邦信息安全管理法》的要求保持一致。

(7) 与 2002 年《电子政府法》相一致，首席信息官委员会将成为首要的跨机构论坛，改进联邦各部局实施的与信息资源有关的下述工作：设计、采办、开发、现代化、使用、运行、共享和执行。

(8) 交通部和国土安全部将在所有与运输安全和运输基础设施保护有关的事项上展开合作。交通部负责国家航空系统的运营。两个部将联合管制危险材料以任何方式（包括管道）的运输。

(9) 所有的联邦部局应同关系到其职责的（关键基础设施）部门合作，减少恐怖主义之外的其他原因导致的灾难性后果。

在必要时，所有的联邦部局的领导均将与国土安全部长相协调并合作，履行对他们自己的关键基础设施和重要资源的保护职责。

所有的联邦部局的领导应负责他们各自的内部关键基础设施和重要资源的标识，负责对其排列优先级、评估、改良和保护。在与 2002 年《联邦信息安全管理法》保持一致的前提下，各机构将确立并提供信息安全保护，所提供的保护应与信息一旦遭到非授权入侵、使用、泄露、中断、修改或破坏而产生的风险和危害程度相一致。

## 8. 与私营部门协调

国土安全部以及联邦特定机构将根据可适用的法律或规章而与相应的私营部门实体展开合作，不断鼓励发展信息共享和分析机制。此外，国土安全部以及联邦特定机构还应与私营部门合作，不断支持部门协调机制：

- (1) 以标识关键基础设施和重要资源，并为之排列优先级，提供保护；
- (2) 以促进有关物理和信息威胁、脆弱性、事件、可能的保护对策以及最佳措施等信息的共享。

## 9. 国家特殊安全事件

经与国土安全委员会协商后，国土安全部长应负责将某些安全事件指定为“国家特殊安全事件”（NSSE）。本令取代了以前有关 NSSE 的总统令中与此不一致的内容。

## 10. 实施

根据 2002 年《国土安全法》，国土安全部长应该制定一个有关关键基础设施和重要资源保护的全面、综合的国家计划，并在计划中列举国家的目标、目的、里程碑以及自本令发布时起一年内的重点工作。除了国土安全部长认为与国土安全有关的其他内容外，国家计划还应包括如下内容：

(1) 用来标识关键基础设施和重要资源、排列优先级并对保护工作加以协调的战略，包括国土安全部准备如何与联邦其他部局、州和地方政府、私营部门、外国政府以及国际组织合作的战略。

(2) 摘要描述为实现下列目标而准备进行的工作：定义关键基础设施和重要资源、排列关键基础设施和重要资源的优先级、减少关键基础设施和重要资源中的脆弱性、协调对关键基础设施和重要资源的保护。

(3) 摘要列出在与州和地方政府、私营部门共享关键基础设施和重要资源的信息以及向其提供威胁预警数据方面的工作。

(4) 在必要时与联邦的其他应急管理和战备工作，包括国家响应计划和可适用的国家战备目标相协调和整合。

国防部长应在符合 2002 年《国土安全法》以及其他可适用的规定和总统令的前提下建立合适的系统、机制和流程，以及时的方式共享联邦其他部局、州和地方政府以及私营部门中与关键基础设施和重要资源威胁及脆弱性有关的国土安全信息。

国土安全部长将与原子能管制委员会不断合作，且必要时要与能源部合作，以确保：

(1) 保护商业核反应堆——用于核电站的反应堆以及用于研究、试验和训练的非核电反应堆；

(2) 保护医疗、工业和学术装置及设备中用来制造核燃料的核材料；

(3) 保护核材料及废料的运输、存储和销毁。

经与科技政策办公室主任相协调，国土安全部长应每年制定一份联邦研究和开发计划，支持本令的实施。

国土安全部长将与其他必要的联邦部局合作，在与可适用的法律相一致的前提下开展一项地球空间计划，利用商业卫星、空间系统以及其他机构中已有的系统来勘探、绘制、分析、区分关键基础设施和重要资源。国家的技术手段应被看作最后的依靠之一。经与中央情报局局长、国防部长和内政部长、联邦其他部局的领导相咨询，国土安全部长应确立实现该项工作的机制。必要时，司法部长应提供法律建议。

国土安全部长应利用现有的能力来对恐怖分子在攻击关键基础设施和重要资源时可能造成的影响进行综合性的建模，在需要时，还要发展新的能力来开展这项工作。工作的重点在于人口密集区域。拥有相关建模能力的机构应与国土安全部长合作，确立合适的机制来完成本项任务。

为保护基础设施，国土安全部长将建设一个国家级的迹象发现和预警体系结构，并发展国家级的预警能力，以促进：

(1) 对基础设施的基本运行状况形成了解；

(2) 发现攻击行为的前兆；

(3) 形成能够检测和分析可能的攻击模式的浪涌能力<sup>①</sup>。

在建设这样一个体系结构的过程中，国土安全部长将与联邦、州、地方政府以及非政府实体合作，以便对物理和信息基础设施及重要资源形成综合的观点。

在 2004 年 7 月之前，联邦各部局的领导应针对他们所拥有和运行的关键基础设施及重要资源制定保护计划，并提交给 OMB 主任，以待批准。这些计划中涉及标识、优先级、保护以及应急计划，包括如何对基础能力进行恢复和重建。

特定联邦机构每年均应向国土安全部长汇报对各自负责的部门内的关键基础设施及重要资源进行标识、排列优先级以及协调保护工作时的情况。自本令发布起一年内，各机构应提交这些报告，自此以后每年汇报一次。

总统国土安全助理和总统国家安全事务助理应对关系到体系结构的整合以及下一代体系结构的国家安全和应急战备通信政策进行审查，并与合适的联邦部局的领导相协商。自本令发布起 6 个月，总统国土安全助理和总统国家安全事务助理应提交对这类政策的修改建议，供总统考虑。

本令取代了 1998 年 5 月 22 日发布的第 63 号总统令（《关键基础设施保护》）以及本令之前的任何法令中出现的 inconsistent 的内容。而且，总统国土安全助理和总统国家安全事务助理应联合起草一份总统令供总统考虑，以便修改此前发布的总统令，使它们与本令相吻合。

本令仅旨在改进联邦政府行政部门的内部管理，不拟也不会法律或正义角度制造任何会对美国及其各部局或其他实体、其官员或雇员以及任何其他个人造成触犯的权利或利益，不论是在实体方面还是在流程<sup>②</sup>方面。

——布什

① “浪涌能力”（surge capacity）来自于电工学。浪涌也叫突波，指超出正常工作电压的瞬间过电压，常由大型负载设备关闭或雷击引起。国外多在医疗体系中引入该词，指发生大规模地区性疾病时医院对突然激增的病人的诊治能力。近年来已常见于反恐文献中，指危机时的处理能力（通常通过应急人员的数目及能力来表示）。本处指在发生可能的攻击时具有足够的检测和分析能力，不致措手不及。——译者注

② “实体法”（substantive law）与“程序法”（procedural law）是法学词汇，两者是法律体系的两类基本组成。实体法通过对于权利义务的分配和规定，调整最为基本的社会关系；程序法则通过特定的程序规定，确保实体法得以实现。换言之，实体法是规定人们在政治、经济、文化和社会生活等实际关系中的权利和义务的法律，如宪法、刑法、民法、行政法等；程序法是规定实现实体法过程中有关诉讼程序或手续的法律，如刑事诉讼法、民事诉讼法、行政诉讼法等。——译者注

---

## 二十、第 54 号国家安全总统令：国家网络安全 安全综合计划（节选）

美国白宫

2008 年 1 月

---

## 译者注：

第 54 号国家安全总统令同时也是第 23 号国土安全总统令。该令为机密文件，因涉及巨额投资，且一些项目与监控有关，美国国会和社会各界一直要求联邦政府将其公开。在这一压力下，美国政府最终提供了解密版，但仍有大量信息始终未公开。此处的翻译是解密版的主要内容。

## 1. 可信互联网连接

通过可信互联网连接把联邦的企业级规模的网络作为一个单一的网络组织进行管理<sup>①</sup>

可信网络连接活动由管理和预算办公室（OMB）及国土安全部领导，涉及对联邦政府的外部访问点（包括连接互联网的访问点）进行整合。整合后将实施一套统一的安全解决方案，包括减少外部访问点、建立基线安全功能以及对各机构符合这些安全功能的情况进行验证。在可信互联网连接（TIC）活动中，各机构或者作为 TIC 访问提供商（只有数量有限的机构可以自己拥有这种能力），或者通过总务管理局的 NETWORX 合同制度与商业化管理的可信 IP 服务（MTIPS）提供商签订合同。

## 2. 爱因斯坦 2 项目

部署一个由遍布整个联邦的感应器组成的入侵检测系统

入侵检测系统使用的是被动的感应器，当非授权用户试图访问联邦网络时可以做出识别，这构成了美国政府网络防御体系极为重要的部分。国土安全部正在部署一批基于特征的感应器，能够对进入联邦系统的互联网流量进行检查，以发现非授权的访问和恶意的内容，这是爱因斯坦 2（EINSTEIN 2）活动的一个组成部分。爱因斯坦 2 使用了基于特征的入侵检测技术，可以通过分析网络的流量信息来查找可能的恶意活动，这是通过对进出美国政府网络的流量自动进行全封包检查来实现的。与技术上的投入相关的是人力的相应投入，要实现国土安全部已然增多的网络安全使命，就离不开这些人。当联邦网络流量中出现恶意或可能有害的活动时，爱因斯坦 2 能够向 US-CERT 提供实时报警，并对导出数据提供关联和可视化能力。在爱因斯坦 2 的帮助下，US-CERT 的分析人员已经大大提高了对网络环境的理解，增强了查找联邦网络安全缺陷和漏洞的能力。由此，US-CERT 拥有了更强的态势感知能力，可以更有效地形成安全相关信息并在美国政府的网络防护者以及私营部门安全专家、美国公众间更及时地共享这些信息。国土安全部隐私办公室已经对爱因斯坦 2 项目实施了隐私影响评估，并发布了报告。

---

<sup>①</sup> 这里的“企业级”网络与“企业”无关，是从规模上对网络做出的一种描述，由地理上分散的多个局域网络通过专用线路或公用数据网络互联而成，处于同一组织的管辖之下。——译者注

### 3. 爱因斯坦 3 项目

寻求在整个联邦范围内部署入侵防御系统

本项活动代表了联邦行政机关内各民事部门安全防护的下一步发展方向。它称为爱因斯坦 3 (EINSTEIN 3)，其将采用商业技术和专门为政府开发的技术来对进出行政机关网络的流量实施实时的全封包检查，并实现基于威胁的决策。爱因斯坦 3 的目标是发现恶意的网络流量并对其进行特征化表示，以增强网络安全分析、态势感知和安全响应能力。它能在网络威胁造成损害之前对其自动检测并正确响应，因为入侵防御系统支持动态防御。在防范、检测和减少联邦行政部门网络和系统中的漏洞方面，爱因斯坦 3 将向国土安全部的 US-CERT 提供协助。爱因斯坦 3 还为国土安全部提供了对检测到的网络入侵企图进行自动报警的能力，这增强了 US-CERT 与联邦各部门之间的信息共享。如国土安全部认为有必要，就可以将不含通信内容的报警信息传送给国家安全局 (NSA)，国家安全局随后可履行法律授权的职能，从而对国土安全部的工作提供支持。这一活动需要大量和长期的投入来增强国家情报能力，使其能够发现有关外国网络威胁的重要信息并实时将发现的情况通知爱因斯坦 3。国土安全部将能够对国家安全局通过外国情报工作以及国防部在信息保障使命中发现的威胁特征进行采用，并输入到爱因斯坦 3 系统中，以支持国土安全部的联邦系统安全使命。对网络入侵信息的共享将遵循法律的要求，并接受对国土安全、情报和国防相关活动的监督，以保护美国公民的隐私和权利。

国土安全部目前正实施一项演习，该演习基于国家安全局开发的技术，旨在试验这项活动对爱因斯坦 3 提出的能力要求，并实现对民事行政部门系统中网络入侵行为信息的管理和保护工作的制度化。为了在爱因斯坦 3 的设计和运行部署中建立合适和必要的隐私保护机制，政府的公民自由和隐私官员正在与国土安全部和 US-CERT 密切合作。

### 4. 研发

对研发工作进行协调并重新定向

没有一个单独的个人或者组织能够了解政府资助的所有网络相关研发工作。本项活动旨在为协调美国政府资助或实施的网络研发工作而制定战略和组织架构，无论是涉密还是非涉密研发，并在必要时对这些研发工作重新定向。当我们在确定战略投资时，这一活动对于减少联邦资助的网络安全研究项目中存在的重复性、查找研究空白、安排研发工作的优先级以及确保纳税人的钱花得物有所值都至关重要。

### 5. 态势感知

把当前的各网络行动中心相互连接起来，加强态势感知

要确保在政府信息安全办公室和战略行动中心之间共享有关联邦系统中恶意行为的数据，这一需求日趋加大，以便更好地理解政府系统面临的全部威胁，最大化地发挥每个组织的专门能力来打造尽可能完善的国家整体网络防线，同时还要遵循个人隐私和其他信息保护的要求。

为了实现和支持对态势感知的共享，本项活动向承载美国网络活动的 6 个网络行动中心提供了必要的关键手段。这项工作关注的主要方面是，要能够使美国网络活动的各个单元在履行工作使命时做到互为关联，必不可少的内容有：基础功能与投资，如基础设施的改造、带宽的增加以及行动能力的整合；提高协同能力，包括一致的技术、工具和流程；通过共有的分析和协同技术来加强态势感知的共享。

本项活动中，国土安全部的国家网络安全中心（NCSC）将在保护美国政府网络与系统安全中扮演重要角色，它能协调和整合来自 6 个行动中心的信息，做出跨域的态势感知，分析和报告美国网络与系统的状态，以及推动跨部门的协同与协调。

## 6. 反情报计划

制定和实施一个覆盖整个政府部门的反网络情报计划

为了协调联邦所有部门间的有关工作，一个覆盖整个政府的反网络情报计划是必要的，以检测、威慑、消除那些由国外发起的、针对美国及其私营部门信息系统的网络情报威胁。为此，这个计划要确立和扩展反网络情报教育和意识项目，建立人才队伍，以便将反情报融入所有的网络行动和分析之中，提高雇员对反网络情报威胁的认识，提高政府各部门间反情报的协同。《反网络情报计划》与《2007 年美国国家反情报战略》保持一致，并支持 CNCI 中其余的活动。

## 7. 涉密网安全

增强涉密网络的安全

涉密网络中存储着联邦政府最敏感的信息，支持着至关重要的战争、外交、反恐、执法、情报和国土安全行动。对涉密网络的成功渗透或破坏将对我们的国家安全造成极端严重的危害。我们需要恪尽职守，确保涉密网络及网络中数据的完整性。

## 8. 网络安全教育

扩大网络安全教育

为了保护美国政府网络空间的安全，已经有数十亿资金投入到了新技术之中。与此同时，需要有掌握正确的知识、技巧和能力的人来实现这些技术，他们将决定成功与否。然而，目前在联邦政府或私营部门内都没有足够的网络安全专家来实施 CNCI，也没有充分建立起联邦网络安全职业域。现有的各个网络安全培训和人才发展项目尽管不错，但在侧重点方面还有不足，且缺少一致性。为了有力确保我们持久的技术优势以及未来的网络安全，我们必须建立起一支技术熟练、熟谙网络安全知识的人才队伍，以及有效的后续雇员输送通道。为了应对这一挑战，需要制定一个国家战略，就像 20 世纪 50 年代的科学和数学教育改革一样。

## 9. 新技术

定义和制定能“超越未来”的持久的技术、战略与规划

CNCI 的一个目标是发展相关技术，使之能够提高当前不计其数的系统的安全性，并且能在未来 5~10 年内得到部署。本项活动力图制定有关的战略和规划，在政府的研发组合中加大那些具有高风险/高回报性质的关键网络安全问题解决方案的比重。联邦政府已经着手为研究界列举重大挑战，以期帮助解决这些需要创造性思维的困难问题。政府正在识别并与私营部门交流共有的需求，这些需求将驱动双方在关键研究领域的共同投资。

## 10. 网络威慑

定义和发展持久的威慑战略与项目

在一个依赖于有保障地利用网络空间的世界中，我们国家的高层决策者必须仔细考虑美国的长期战略选择。目前，美国政府已经采取了传统的办法来解决网络安全问题，这些措施还没有达到我们需要的安全水准。本项活动旨在建立一种实现网络防御战略的方法，通过完善预警能力、发挥私营部门和国际合作者的角色、对来自国家和非国家的行动者进行正确应对，威慑对网络空间的干涉和攻击。

## 11. 供应链安全

建立全方位的方法来实施全球供应链风险管理

商用信息和通信技术市场已经全球化，这为那些试图通过渗透进供应链来非授权访问数据、篡改数据或拦截通信信息，从而危害美国的人们提供了更多的机会。必须采用能够涵盖产品、系统和服务的完整生命周期的战略性、综合性的方案，对来自国内和全球供应链的风险加以管理。这种风险管理要求对威胁、漏洞以及采购决定的后果具备更强的意识，要求开发和部署能在产品的生命周期内（从设计到报废）从技术和操作层面减少风险的工具和资源，要求建立能够适应复杂的全球化市场的新采购政策和实践措施，要求与工业界合作制定和采用供应链与风险管理标准及最佳实践措施。本项活动将使联邦政府向各部门提供强健的供应链风险管理与控制工具集的能力、政策和流程得到强化，使经过管理和控制后的供应链风险同系统与网络的重要性相称。

## 12. 联邦在关键基础设施安全中的角色

明确联邦的角色，使网络安全延伸到关键基础设施领域

美国政府要依赖大量由私营机构拥有和运行的关键基础设施来完成公共事务。这些关键基础设施离不开信息系统和网络的高效运行，而这些系统和网络都易遭受恶意的网络威胁。本项活动建立在已有且不断发展的合作关系基础之上，合作关系的一方是联邦政府，另一方是位于公共和私营部门的关键基础设施与重要资源（CIKR）的所有者、运营者。国土安全部及其私营部门的合作者已经制定了一项共同行动的计划，包括一系列里程碑及行动。计划中既有短期的建议，也有长期的建议，特别是融入并充分利用了以前的成果和行动。它考虑了整个网络空间基础设施的安全和信息保障工作，以增强所有 CIKR 领域的韧性和运行能力为目的。其侧重点之一是公共-私营之间就政府以及 CIKR 领域网络威胁和事件信息的共享。



---

## 二十一、网络空间政策评估：保障可信和坚韧的信息和通信基础设施

美国白宫  
2009 年 5 月

---

## 序

网络空间通达万物，影响诸人。其提供了创新与繁荣的平台，提供了增进全球福祉的途径。但是由于管控松弛的数字基础设施已经广泛渗透，各种巨大的风险正在对国家、私营企业和个人权利构成威胁。美国政府有责任解决这些战略脆弱性，确保美国及其公民能与世界更多的国家一起，使信息技术革命的潜能得到全面发挥。

主要以互联网为基础的国家数字基础设施的架构并不是安全和坚韧的。如果这些系统在安全上没有取得重大进展，或在如何构建和运营上没有实现重大改观，就会让人怀疑美国能否保护自己，不受网络犯罪及有国家支持的入侵和作战行动的日益威胁。我们的数字基础设施早已遭受到入侵，犯罪分子已经窃取了亿万美元，一些国家和其他实体盗取了知识产权和敏感的军事信息。还有的入侵可能会损坏我们部分关键基础设施。这些风险以及其他风险有可能会动摇国家对信息系统的信心，而正是这些信息系统支撑了美国的经济和国家安全利益。

联邦政府还没有组织起来有效地解决这个在当前及今后都日益严重的问题。网络安全责任分散在不同的联邦政府部、局之间，很多是职能交叉，没有一个部门拥有足够的决策权来指挥行动，并协调一致地去处理相互矛盾的问题。政府需要综合考虑各方的竞争性利益，制定出一个全面愿景和计划，以解决美国面临的网络安全问题。国家需要制定出必要的政策和程序，培养人才，发展技术，以降低网络安全相关风险。

无论是在美国国内还是在国际上，信息和通信网络绝大多数是归私营部门拥有并运营的。因此，解决网络安全问题需要政府和私营部门之间的伙伴关系，以及国际合作和国际准则。美国需要拥有一个全面的架构，以确保政府、私营部门和我们的盟国在发生重大网络事件或威胁时，能够协调一致地响应和恢复。

美国需要开展一次全国性的网络安全讨论，更多地提升公众对网络威胁与风险的意识，以确保拥有一套完整的办法来满足国家对网络安全的需要，并履行国家对受宪法和法律保护的隐私权、公民自由的承诺。

对信息和通信基础设施安全和韧性的新方法研究十分不足。政府需要加大研究经费投入，以解决网络安全脆弱性问题，同时也能满足我们经济和国家的需要。

## 执行摘要

总统指示，要在 60 天内全面、全新地评估美国网络安全政策和架构。网络安全政策包括网络空间安全和运行的战略、政策及标准，涵盖了所有与减轻威胁、减少脆弱性、威慑、国际接触、应急反应、韧性及恢复有关的政策与行动，并包括计算机网络运行、信息保障、执法、外交、军事和情报任务等，它们与全球信息和通信基础设施的安全与稳定息息相关。评估报告研究的内容并不包括与国家安全或与基础设施安全无关的其他信息与通信政策。由政府网络安全专家组成的评估小组汇总了产业界、学术界、公民自由与隐私团体、州政府、国际合作伙伴以及立法和行政部门提出的看法。本文概述了评估小组的主要结论，并描绘了在未来如何实现可靠、富有韧性和可信的数字基础设施。

### 美国正处在十字路口

全球互联的数字信息和通信基础设施被称为“网络空间”，其支撑了现代社会的方方面面，提供了对美国经济、民用基础设施、公共安全和国家安全的关键支撑。这项技术已经使全球经济发生了改变，使人们以难以想象的方式联系在一起。然而，网络安全的风险也成为美国在 21 世纪某种最严峻的经济和国家安全挑战。数字基础设施的体系结构更多地受到互操作性和效率的驱使，而不是从安全的角度进行考量的。于是，越来越多的国家和非国家行为体开始损毁、盗窃、篡改或破坏信息，这将为美国的系统带来重大破坏。与此同时，传统的电信和互联网持续融合，而其他基础设施部门正将互联网作为主要的互联手段。美国面临着双重挑战，既要维护促进高效、创新、经济繁荣和自由贸易的良好环境，又要确保平安、安全，维护公民自由和隐私权<sup>①</sup>。解决网络空间的战略脆弱性，并确保美国和世界充分实现信息技术革命的潜能，这是我们政府的一个基本责任。

### 再也不能容忍目前的状况

美国必须向世界表明，美国将凭借强有力的领导和愿景，严肃认真地迎接这一挑战。白宫内部的领导力应得到提升并强有力地确定下来，以提供指导，协调行动，并取得成效。此外，要落实联邦政府网络安全的领导力和责任制。这要求清晰描述联邦政府各部、局的网络安全相关角色和职责，同时为其提供相关政策、法律架构和必要的协调，便于各部门能够实现其使命。在过去的两年中，我们已经开始实施重大的计划，并通过将各机构此前各不相干的使命进行“衔接”而取得了长足的进步，但这仍是不完整的解决方案。此外，这一问题超越了各个政府部、局的管辖范围。尽管每个部、局在网络安全方面都发挥着不可替代的作用，但任何一个部门都不具备足够广阔的视野或足够的授权来彻底解决这个问题。

### 立即启动全国网络安全大讨论

美国政府应该与业界共同向民众解释清楚这个挑战，并讨论国家将如何通过一种让美国人民认可行动必要性的方式来解决面临的问题。人们若不先了解网络问题的风险程度就不可能重视网络安全。因此，联邦政府应借鉴以往成功的经验，发起一个全国性的公众意识和教育运动。此外，与 1957 年 10 月苏联发射第一颗人造地球卫星后的一段时间类似，我们正面临一场全球数学和科学技能竞赛。虽然我们继续拥有世界上最良好的信息技术产业环境，但同时国家应培养参加全球竞争并保持领导地位所必需的人才队伍。

### 孤军奋战不可能成功保护网络空间安全

美国政府应加强与私营部门的合作。公共-私营部门的利益是交织在一起的，对确保安全、可靠的基础设施负有共同责任。联邦政府有很多可以与私营部门合作的方法，应当去努力探寻。网络安全领域的公共-私营合作关系必须得以发展，以清晰地界定这种关系的性质，包括明确各自的角色和职责<sup>②</sup>。联邦政府应审查现有的公共-私营合作关系，优化其确定优先级的能力，

① 互联网安全联盟《网络安全社会合约：对奥巴马政府和第 111 届国会的政策建议》，第 5 页。

② 微软公司 Scott Charny 在众议院国土安全委员会新威胁、网络安全和科技子委员会上的证词，2009 年 3 月 10 日，第 4 页；跨部门网络安全工作组（CSCSWG）对 60 天网络安全评估报告有关问题的回应，2009 年 3 月 16 日，第 2 页；信息技术和通信部门协调委员会，2009 年 3 月 20 日，第 2 页。

使各项具体行动得到高效执行<sup>①</sup>。

美国还需要制定一个网络安全战略，以塑造国际环境，使志同道合的国家就涉及领土管辖权、主权责任和使用武力的有关技术标准和可接受的法律规则等一系列问题达成共识。国际规则对于建立安全和繁荣的数字基础设施是至关重要的。此外，各个国家和地区相异的法律规定和做法，如网络犯罪调查与起诉，数据保存、保护和隐私权，网络防御和事件响应方法等方面，有很多相关的法律，这给实现平安、安全和可信的数字环境带来了严重挑战。只有通过与国际合作伙伴的共同努力，美国才有可能更好地应对这些挑战，加强网络安全，并全面享有数字时代带来福利。

**在保护国家免受网络事件或事故方面，联邦政府既不能将职能完全下放，也不能放弃职责**

联邦政府担负有保卫国家的责任，各级政府担负着确保公民安全和福祉的责任。但是，私营部门设计、建造、拥有并运营着大部分的数字基础设施，支撑着政府和私人使用者。美国需要有一个全面的框架方案，以确保联邦、州、地方和部落政府、私营部门和国际盟友能够对重大事件做出协调一致的反应。实施这一框架需要为事件报告制度确定阈值，制定可适应性的应急计划和灾难恢复计划。为了成功实施这些计划，还要设计必要的协调、信息共享和事件报告机制。政府应在与主要利益相关方共同努力下，设计一个有效的机制以实现真正共同运作的构想，整合政府和私营部门的信息，并以此为基础将已周知各方且已排列优先级的脆弱性削减工作及事件响应决策工作向前推进。

**与私营部门合作，明确下一代基础设施的性能和安全目标**

美国应充分利用技术优势满足国家经济和国家安全需要。即使面对老练敌人的攻击，联邦政府制定的政策也应能够满足国家安全、知识产权保护及基础设施可用性和连续性等需求。通过与私营部门、学术界的合作，联邦政府需要清楚地阐明其协调一致的国家信息和通信基础设施的目标。应与州和地方政府合作，制定有效的采购战略，推动市场制造更安全的产品并为公众提供各种有效的服务。政府还应探索另外的一些激励机制，包括调整法律责任（提升安全可以减责，安全糟糕则导致责任增加）、补偿金、税收优惠以及新的监管要求和合规性机制等<sup>②</sup>。

**白宫必须领导前方之路**

在过去 15 年里，国家采取的网络安全措施没能跟上威胁的发展变化。我们需要向国内外证明，美国是在认真地对待网络安全相关的问题、政策和活动。这就要求由白宫挂帅，汇集整个国家的力量、建议和思路。

本评估报告建议了如下的近期行动计划：

1	任命一名网络安全政策官，负责协调全国的网络安全政策和活动；建立一个强大的国家安全委员会的网络安全指挥部，受网络安全政策官的指导，并向国家安全委员会和国家经济委员会报告，以协调部门间对网络安全有关战略和政策的制定
2	为总统起草新版的保护信息和通信基础设施的国家战略，这一战略应包括对 CNCI 活动的持续评估，必要时延续 CNCI 已经取得的成功
3	将网络安全作为总统的关键管理优先事项并制定业绩指标

① 战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 43 页；TechAmerica 对 60 天评估的回应，第 6 页；商业软件联盟《国家安全和国土安全委员会对国家网络安全政策的审视》，2009 年 3 月 19 日。

② Cato 学会，Jim Harper 文章《政府使网络安全了吗？》，2009 年 3 月 13 日；互联网安全联盟《行为准则——哈萨维的问题》，2009 年 3 月 24 日，第 2、4~7 页。

续表

4	在国家安全委员会的网络安全指挥部指定一名负责隐私和公民自由的官员
5	召集政府相关机构，就在制定政策过程中遇到的网络安全相关事宜进行清除跨越部门界限的法律分析研究，并制定统一的政策指导，以明确政府各部门网络安全工作的任务、职责和权限
6	发起一场促进网络安全公众意识的全国性教育运动
7	确定美国政府对国际网络安全政策框架的立场，加强我们的国际伙伴关系。针对网络安全有关的各类活动、政策制定和机会，主动作为
8	制定网络安全事件响应计划；展开对话，以加强公共-私营合作关系，着眼于理顺关系，并提供资源，便于其贡献和参与
9	与其他总统行政办公室（EOP）实体合作，制定研发战略框架，侧重于以改变游戏规则的有潜力的技术，以提高数字基础设施的安全性、可靠性、韧性和可信度；为研究界提供获得事件数据的途径，便于其开发工具、测试理论，并找出可行的解决方案
10	建立一个网络安全的身份管理的愿景和战略，以解决隐私和公民自由的关切，利用隐私增强技术保卫国家

## 引言

全球相互连接的数字信息和通信基础设施被称为“网络空间”，其几乎支撑了现代社会的各个方面，为美国经济、民用基础设施、公共安全和国家安全提供了重要的支持。信息技术已经改变了全球的经济，并超乎想象地把人和市场连接在一起。为充分享用数字革命带来的好处，用户必须能够确信敏感信息得到保护，商业活动不会受到破坏，基础设施不会遭到入侵。各国也需要树立信心，相信支持其国家安全和经济繁荣的网络是安全的、富有韧性的。拥有可信的通信和信息基础设施将会确保美国充分发挥信息技术革命的潜能。第 44 届总统网络安全委员会在 2008 年 12 月的报告中明确指出：“美国网络安全保护不力是新一届美国政府所面临的最紧迫的国家安全问题之一。”<sup>①</sup>

### 什么是网络空间？

第 54 号国家安全总统令/第 23 号国土安全总统令将网络空间定义为：信息技术基础设施相互依存的网络，包括互联网、电信网、计算机系统以及重要工业中的嵌入式处理器和控制器。该词的常见用法还指人与人之间通信及交互的虚拟环境。

保护网络空间需要具有远见卓识和强有力的领导，需要在政策、技术、教育乃至法律等方面进行变革。政府最高领导层、产业界和公民社会要共同展现对网络安全相关事项的承诺，这会使美国在增强国家安全和全球经济的同时，继续创新和尖端技术运用方面保持领先地位。

### 为什么要行动

网络威胁是 21 世纪美国和其盟友面临的最严重的经济和国家安全挑战。越来越多的国家和非国家行为体，如恐怖分子和国际犯罪集团，开始把攻击目标对准了美国的公民、商业、关

① 战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 11 页。

键基础设施和政府。他们有能力损毁、窃取、篡改或完全破坏信息<sup>①</sup>。持续非法利用信息网络和破坏敏感数据等行为，特别是由国家实施的行动，使美国经济竞争力和军事技术优势面临损失。正如国家情报总监最近在国会作证时所陈述的那样：“信息系统、互联网和其他基础设施之间越来越多地互联，为攻击者破坏电信、电力、能源管道、炼油厂、金融网和其他关键基础设施创造了机会。”情报界评估认为，一些国家早已拥有了实施这种攻击的技术能力<sup>②</sup>。

日趋复杂、广泛的犯罪活动，以及网络事件已经造成的危害，凸显了网络空间中恶意行为有能力影响美国竞争力、损害隐私和公民自由、破坏国家安全或打击公众信心，甚至使社会瘫痪。例如：

- 关键基础设施失去运转能力。中央情报局报告指出，针对 IT 系统的恶意活动已经使海外多个地区的供电设施遭到破坏。在其中一起案例中，恶意行为曾导致多个城市断电<sup>③</sup>。
- 破坏全球金融服务。据新闻报道<sup>④</sup>，2008 年 11 月，一家国际银行付款处理器遭到破坏，导致遍布 49 个城市的 130 多台自动取款机非正常交易达半小时之久。在媒体报道的另一起案件中，一家美国零售商在 2007 年遭遇了数据被破坏和个人身份识别信息丢失的事件，殃及 4500 万张信用卡和借记卡<sup>⑤</sup>。
- 美国经济利益遭受全面损失。业界估计，在 2008 年，知识产权与数据失窃给美国造成了高达 1 亿美元的损失<sup>⑥</sup>。

本报告中使用的“网络安全政策”包括网络空间安全和运行的战略、政策和标准，涵盖了全面降低威胁、减少脆弱性、实施威慑、国际接触、事件响应、韧性、恢复政策及行动，包括计算机网络运行、信息保障、执法、外交、军事和情报活动，它们与全球信息和通信基础设施的安全与稳定息息相关，但并不包括与国家安全和基础设施安全无关的其他信息和通信政策。

### 全新的评估

认识到挑战与机遇，总统将网络安全确定为本届政府的优先议题，并指示尽早进行 60 天的全面审查，评估美国网络安全政策与架构。这一评估针对的是信息和通信基础设施有关的所有任务和活动，包括计算机网络防御、执法调查、军事与情报活动以及与之有关的信息保障、反情报、反恐、电信政策和综合的关键基础设施保护等方面内容。由政府网络安全专家组成的评估小组全面评审了相关的总统政策令、行政令、国家战略和政府顾问委员会及私营部门实体提供的研究报告。评估小组还向政府各部、局征求了意见，请它们按要求就各自与网络安全相关的具体活动、授权和能力提供材料，并要求政府各部、局标识那些可能没有列入最初清单之

① 国家情报主任《情报共同体对众议院军事委员会的年度威胁评估，记录版》，2009 年 3 月 10 日，第 39 页。

② 同①，第 39~40 页。

③ [www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5](http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5)，SANS 的 SCADA 峰会上中情局的报告，2008 年 1 月 16 日。

④ [www.bankinfosecurity.com/article.php?art\\_id=1197](http://www.bankinfosecurity.com/article.php?art_id=1197)，2009 年 2 月 5 日。

⑤ [www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952](http://www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952)，2007 年 1 月 17 日。

⑥ [www.mcafee.com/us/about/press/corporate/2009/20090129\\_063500\\_j.html](http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html)，McAfee 报告《不安全的经济：保护虚拟信息》，2009 年 1 月，基于普度教育和研究中心的信息保障和安全调查项目。

中的新需求或已存在的需求。于是，很多法律问题浮出了水面。例如，授权集中问题；政府在保护私人拥有的关键基础设施方面应当有什么样的权限；互联网监控软件的安装；自动化攻击检测和预警传感器的应用；联邦政府与第三方数据共享；对私营部门的保护责任等。

评估小组还走出去，与联邦政府内外的广大利益相关方进行了沟通。评估小组力争透明，与产业界、学术界、公民权利与隐私社团、州政府、国际合作伙伴以及立法和行政部门广泛沟通，标识与评估其他的相关的项目和事务。评估小组认识到，每个人包括学术界、产业界和政府都面临机会，一起努力建立可信和有韧性的通信和信息基础设施，小组为此将这些利益相关方纳入评估工作的范畴，请它们就涉及的领域提供材料。这种沟通工作包括 40 多次会议，形成了 100 多份带有具体建议和目标的文件。各利益相关方的反馈和公开评论（如国会证词）等有助于确定重大需求，指明政策差距，提出改进或合作的领域，并为网络安全相关政策的决策提供了框架。

评估小组发现，在整个信息和通信基础设施发展过程中，法律和政策当时是为管理多样化和分散的技术及产业而制定的，各部、局的任务与职权则是这些法律和政策赋予。而由此产生的各项工作主要是用于处理当时的特定问题或技术，未必适应今天对数字化信息高度依赖的现实。

技术对国家和经济安全的影响促使联邦政府做出变化，设定新的法律和组织机构。例如：

- 在 1918 年的一个联合决议案中，国会授权总统掌控美国所有电报系统，确保在第一次世界大战期间能够运转。
- 1934 年，《通信法》决定将联邦无线电委员会调整为联邦通信委员会，并为所有的通信，无论是有线还是无线，建立了全面管制框架，对此类技术的后续发展产生了深远影响。
- 1965 年，《布鲁克斯法》规定国家标准局（NBS），如今是商务部的国家标准与技术研究院（NIST）负责制定自动数据处理标准和联邦计算机系统相关指南。
- 1984 年，第 12472 号行政令将美国国家通信系统（NCS）作为联邦政府拥有或租用的、满足国家安全和应急战备之用的电信财产。2003 年，美国国土安全部继承了 NCS 的管理权。
- 1994 年，美国国务院根据《对外关系授权法》，负责管理与国际通信和信息政策有关的外交政策。

要回答“谁负责”的问题，就必须解决政府部、局间法定授权和使命的分配问题，尤其是在电信和互联网类的网络相互融合，以及其他基础设施部门日益将互联网作为主要的互联手段的背景下。将已经发展了一个多世纪的使命职责统一起来，这就要求联邦政府详细阐明网络安全政策，明确政府各部、局在网络安全方面各自的角色和责任。评估小组对 20 多个联邦政府部、局的反馈意见进行了分析，标识了网络安全相关政策的缺口和职能重叠领域以及改善合作水平的机会。

随着威胁日益复杂，应对网络空间风险的工作以及协调各部、局的工作也在变化。1998 年 5 月签署的第 63 号总统令规定，在白宫的直接领导下设立了一个架构，对指定的部门领导机构进行协调，与相对应的私营部门进行合作，以“消除我们关键基础设施面对物理和网络攻击时的任何重大脆弱性，特别是我们的网络系统”<sup>①</sup>。这项政策在 2003 年的“保护网络空间安

① PDD63《关键基础设施保护》，1998 年 5 月 22 日，第二节。

全的国家战略”文件中又进行了修订。2003年年底的第7号国家安全总统令进一步增强了这项工作。该命令赋予了国土安全部职责，在与行政部门内指定的与各关键基础设施对口的机构的合作下，全面协调各行业的关键基础设施保护，包括网络基础设施<sup>①</sup>。这两项政策的重点是防御性战略，第7号国家安全总统令并未包括保护联邦政府的信息系统。2007年，“国家网络安全综合计划”（CNCI）采取了不同的方法，其核心是把过去分散的网络防御任务与执法、情报、反情报和军事能力“衔接”起来，解决从远程网络入侵到内部违规操作及供应链风险等各种各样的全面威胁。“国家网络安全综合计划”（CNCI）战略在第54号国家安全总统令/第23号国土安全总统令中提出，主要针对行政部门的网络安全，这只是美国所依赖的全球信息和通信基础设施中的很少一部分。

本文总结了评估小组的调查结果，并介绍了有助于美国在未来实现更可靠、有韧性、可信的数字基础设施的一些初步行动领域。它并未对各种选择或诸多工作的审计情况提供深入的分析。相反，它提出了更多的协调需求以及更多的制定综合性政策的需求。本文用五个主题详细地介绍了调查结果和行动选项：一是从顶层加强领导；二是建设数字化国家的能力；三是共同负责网络安全；四是加强信息共享和应急响应；五是构筑未来架构。此外，本文还包括几个附录，包括（1）参考文献；（2）研究所用的方法学；（3）现代通信技术的发展历史<sup>②</sup>。

## 1. 从顶层加强领导

确保网络空间拥有足够的韧性并可信，以支持美国的经济增长、公民自由与隐私保护、国家安全和民主体制的完善，这要把网络安全列为国家头等大事。只有在政府最高层领导下才能完成这一重要而复杂的任务。

### 由白宫实施领导

在白宫层面增强和提升网络安全相关政策的领导权，这会向美国和国际社会发出明确的信号，即我们对网络安全问题的态度是非常严肃认真的。很多政府部、局，以及总统行政办公室将需要协调不同的职责和授权，以有效地促进网络安全。目前，没有一个人或一个实体专门担负着协调联邦政府网络安全相关活动的职责。没有一个中央协调机制，没有新版的国家战略、行动计划，没有各行政部门的协调，没有国会的支持，靠单独的工作不足以应付这一挑战。

政府早已经设立了一个由国家安全委员会和国土安全委员会共同领导的信息和通信基础设施跨部门政策委员会（ICI-IPC），作为解决有关网络问题的主要政策协调机构<sup>③</sup>，以实现可信、可靠、安全和长久的全球信息和通信基础设施及相关能力。

美国总统应该考虑再任命一名白宫网络安全政策官，该官员应向国家安全委员会和国家经济委员会报告，以协调全国范围内与网络安全有关的政策和活动。此官员将主管信息和通信基础设施跨部门政策委员会工作，启动一项强有力的与其他总统行政办公室进行协调的工作，以解决各种彼此冲突的优先任务，协调政府部门间网络安全政策和战略的制定<sup>④</sup>。网络安全政策

① 第7号国土安全总统令《关键基础设施标识、优先级和保护》，2003年12月17日。

② 因篇幅原因，翻译稿未收录这几个附录。

③ 白宫实施的一个独立的60天研究活动正在评估这两个委员会的组织架构，本文以下部分只是简单地提到NSC。

④ 战略与国际研究中心（CSIS）对第44任总统的网络安全建议，2008年12月，第36页。



官应与所有相关的经济、反恐和科技政策的讨论，使它们将网络安全纳入视野<sup>①</sup>。

要取得成功，总统网络安全政策官必须得到总统的全力支持，拥有授权和足够的资源，以便在政策制定和协调跨部门网络安全相关活动时有效地开展工作。其至少有来自国家安全委员会的两名资深主任和相关工作人员的辅佐，并至少有一名国家经济委员会的资深主任和相关工作人员为其工作。这些资深主任应通过网络安全政策官向上汇报工作，并共同致力于达成本报告所设定的目标及其他国家政策。此外，为促进国家安全委员会的整编，委员会中的每个地区主管局和职能局应当专设一名工作人员，负责本单位职能范围内的网络安全事务，并与委员会中的网络安全局协调工作。

网络安全政策官不应拥有运行责任或权力，也没有权力自己制定政策。网络安全政策官应当利用跨机构的协调程序，来协调联邦政府的网络安全相关政策与技术，确保总统的预算能够反映联邦对网络安全的优先级，并制定立法进程，这都要与联邦政府的首席技术官和首席信息官咨询，还要与管理与预算办公室（OMB）、科技政策办公室（OSTP）和国家经济委员会（NEC）等相关部门进行商议<sup>②</sup>。

该网络安全政策官还可作为白宫负责网络事件响应的行动官（其职能与白宫负责监控恐怖袭击和自然灾害的行动官员相类似），因此建立网络安全政策官也将使美国更有效地进行危机管理。政府部门和机构将继续担负各自的网络运营职责。

为了便于协调，所有联邦政府部、局应该在各自内部设立一名联络官，负责协助白宫处理网络安全相关事务。

通过跨部门政策制定程序，网络安全政策官应当为总统起草新的国家战略，以确保信息和通信基础设施安全。这项战略应包括对“国家网络安全综合计划”的落实情况的后继评估，并延续其已取得的成功<sup>③</sup>。新国家战略应使高层领导的注意力和所花费的时间转向如何解决美国面临的障碍，以实现可信、可靠、安全和富有韧性的全球信息和通信基础设施以及相关能力<sup>④</sup>。该战略将帮助政府努力提高公众意识，恢复和建立国际联盟及公共-私营部门之间的伙伴关系，建立一个更加全面的国家网络响应与恢复计划，并积极地推进研发进程，催生提高网络安全的新技术。

联邦政府应继续落实“国家网络安全综合计划”提出的“任务衔接”原则。政府各部、局应加强网络防护者与负责美国网络空间行动能力的情报、军事和执法单位的合作，就网络威胁、谍报、技术和脆弱性等问题进行交流，扩大对经验、知识和观点看法的共享。此外，网络安全政策官应当帮助协调涉及网络空间的情报、军事政策和战略，包括打击网络恐怖主义，确保所有的任务合理融合在一起。网络安全政策官还应当与外部的咨询机构保持联系。很多咨询机构都涉足与网络安全相关的问题，包括国家安全和电信咨询委员会（NSTAC）、国家基础设施咨询委员会（NIAC）、关键基础设施合作咨询委员会（CIPAC）以及信息安全与隐私咨询委员会（IAPAB）。网络安全政策官应审查这些机构的职能，并提出必要的改革建议使其咨询服务最优

① 微软公司 Scott Charny 在众议院国土安全委员会新威胁、网络安全和科技子委员会上的证词，2009 年 3 月 10 日，第 2 页；战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 28 页

② 情报和国家安全协会《网络保障政策改革的主要问题》。

③ 战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 59 页。

④ 跨部门网络安全工作组对 60 天网络评估问题的回应，2009 年 3 月 16 日，第 11 页。

化，并杜绝不必要的重复。

为确保公民自由和隐私权利得到保护，还需要得到其他组织的帮助。这些组织可以在公民自由与隐私团体、公众和政府的网络安全工作之间建立起信任，显示网络安全工作的透明性，这在网络计划开始实施之初尤为重要<sup>①</sup>。当务之急是重新组建隐私与公民自由监督委员会（PCLOB），加快委员会成员的选举工作，并考虑是否通过法律修正案以扩大其工作范围，包括处理与网络安全有关的事务<sup>②</sup>。其他可行的办法还包括：促进政府中负责公民自由事务的部门与隐私顾问们就网络安全的政策问题进行定期沟通，或在国家安全委员会内任命一名负责隐私与公民自由事务的官员（或范围再大一些，在总统行政办公室内任命）以及与私营部门隐私与公民自由团体、隐私与公民自由监督委员会和政府负责隐私与公民自由事务的官员进行协商<sup>③</sup>。

与制定网络安全政策同样重要的是确保其有效地执行和落实，以实现更远的战略目标。因此，网络安全政策官要同管理和预算办公室（OMB）、总统的其他行政办公室协商必须确保有效地落实网络安全相关政策和采取相关行动。在 60 天的评估期间，有关各方就协调和监督网络安全活动提出了各种各样的办法。一些评论者将强有力的行政领导以及各部、局集中、长期的关注，作为确保美国政府拥有有效的网络安全工作机制的重要因素。目前，对现有一些网络安全工作的监督职能超出了总统行政办公室的范围。例如，归属国家情报总监领导的跨部门联合网络任务组（JIACTF），目前负责协调和监督执行《国家网络安全综合计划》的实施。网络安全政策官应通过与管理与预算办公室（OMB）、总统其他行政办公室的咨商，提出组织结构调整的建议，以实现相应的监督、执行和其他的一些职能，包括在 OMB 或总统行政办公室建立一个类似 JIACTF 的机构<sup>④</sup>，创立一个类似艾森豪威尔总统行动协调委员会的实体<sup>⑤</sup>，或建立一些可协助评估联邦政府各部、局表现和监督联邦政府网络安全标准合规情况的组织架构。在这样一个办公室成立之前，JIACTF 将继续执行其任务<sup>⑥</sup>。

### 评估相关法律和政策

总统的网络安全政策官应与各政府部、局合作，提供协调一致的政策指导，并在必要时详细说明整个联邦政府确保网络安全相关活动的权限、角色和责任。适用于信息和通信网络的法律是由宪法、国内法、国外法和国际法拼凑而成的一个复杂法律体系，为政策选项带来了制约。在美国，这种拼凑在一起的法律混合体之所以存在，是因为联邦政府在整个信息和通信基础设施发展过程中，颁布了诸多法律和政策，试图管理非常多样化的产业和技术。

传统的电信网络和互联网类型的网络日益融为一体，其他基础设施领域日益将互联网作为互联的主要手段，法律和政策应当继续探索一种综合性方法，将保护公民自由、隐私权利、公

---

① 电子前线基金会提交给白宫的评估材料，第 1 页。

② 国家安全研究中心致国家安全委员会的信，2009 年 4 月 8 日，第 2 页。

③ TechAmerica 对 60 天网络安全评估的回应，第 6 页；Ari Schwartz 和 Gregory Nojeim（民主和技术中心）致国家安全委员会的信，2009 年 3 月 20 日，第 4~5 页。

④ JIACTF 活动包括评审目标的成果、最近的成绩、所规划的活动和进度、风险和风险削减战略、预算、人事、绩效指标以及各部、局的季度报告中要求的关键事务。

⑤ 10483 号行政令建立。

⑥ 国会研究中心给国会的报告《总统行政办公室：历史的观点》，2008 年 11 月 26 日，第 21 页。

共安全、国家和经济安全的利益与灵活多样的网络应用和网络服务所带来的好处结合起来。在一些领域中缺乏司法裁定，这既带来了机遇，也带来了危险，决策者对此应充分理解，法院可以介入并规范法律的应用，尤其是涉及宪法权的领域。政策决策必然受到法律框架的规范和制约，政策上的考虑也会有助于找出现行法律中存在的差距和争议，以了解法律必须改进的地方。根据美国的宪法原则，这一过程可能会提出新的立法框架，以调整信息、通信、网络和技术领域那些彼此重复的法律，或对已有的法律进行新的解释，使之适应技术变革与实现政治目标。然而，采用其中任何方式都会有风险，可能使联邦政府保护信息和通信基础设施的一些活动更加困难。

政府应适当地与国会进行有效合作，以确保有完备的法律、政策和资源用于支持美国网络安全相关使命。国会已对国家有关网络安全的需求表示关注，并决定由两党共同担任领导，政府将会从国会的知识和经验中获益。政府各部、局共同工作的网络安全政策官应与产业界进行磋商，以便了解法律和政策给企业经营带来的影响。

### 加强联邦对网络安全的领导和责任制

在数字化时代，仅仅依靠白宫将不足以实现带领美国发展的广泛目标，整个联邦政府都必须担负起领导职责。将网络安全列入总统管理活动的优先事务，或根据既定的目标评估政府各部、局的网络安全工作进展等，都有助于落实责任和工作进展。网络安全政策官经与国家安全委员会（NSC）、管理和预算办公室（OMB）、国家经济委员会（NEC）和科技政策办公室（OSTP）协商，将界定里程碑和成功标准，提高网络安全工作在所有机构预算中的“能见度”。

要使网络安全工作透明并对整个网络安全投资进行有效管理，管理和预算办公室（OMB）应利用其工作评估框架，以确保政府各部、局在追求网络安全目标时实施基于效能的预算。正规的网络安全工作评估框架可以使政府各部、局详细说明每项网络安全工作的意图与目标，并建立是否达成目标的统一标准。《国家网络安全综合计划》已经成功地运用了一种类似的做法<sup>①</sup>。

根据 2002 年《联邦信息安全管理法》要求，政府各部、局的领导人必须承担起责任。政府应当与国会共同努力，更新并强化这项立法。政府各部、局的领导的绩效计划应当要求各部、局及时汇报在确保网络系统安全方面的工作进展情况。美国联邦政府应制定方案，使政府各部、局的领导可以为网络安全政策的合规性负责，以强制执行相应的网络安全流程。

### 提升州政府、地方政府和部落政府的领导力

州、地方和部落政府应考虑把网络安全当成一件大事来抓，指定一名领导人专门负责，以确保首席信息官、首席信息安全官与州国土安全顾问之间的有效协调。评估小组从美国州长协会的代表那里听到一些反映，说网络安全是他们在保护各州关键基础设施资产工作中最薄弱的环节<sup>②</sup>。在很多国土安全部批准的项目中，州国土安全顾问可以从中列支资金，用于网络安全工作。但从历史上看，所提供的资金在很大程度上并没有优先用于网络安全。州、地方和部落政府应考虑是否应把网络安全当成一个大问题，并确保首席信息官、首席信息安全官与州国土安全顾问协调一致，实现强有力的防御态势。

① 参见信息基础设施保护协会的《与经济、物理基础设施和人类行为有关的国家网络安全研发挑战：工业界、学术界和政府的视角》，2009 年，第 5、29 页。

② 与州际信息共享和分析中心代表的会谈，2009 年 3 月 6 日；与国家州长协会代表的会谈，2009 年 3 月 25 日。

## 2. 打造数字化国家能力

我国正处于一个十字路口。计算机几乎改变了日常生活的一切，不论是在家中还是工作场所。网上银行、网上购物和报税等都已司空见惯。国家的基础设施正在经历一场革命，数字化和网络技术在大型系统中不断进行整合，如智能电网和下一代空管系统。近期发布的《美国复苏与再投资法》中的内容鼓励发展现代信息和通信基础设施，以便提高美国的竞争能力，并使用技术来解决国家所面临的最为紧迫的问题。美国面临着双重挑战：在维护一个促进创新、开放互联、经济繁荣、自由贸易及自由的环境的同时，也要保证公共安全、公民自由和隐私。

大众需要很好地了解如何安全使用技术。另外，美国需要一支技术先进的人才队伍来维持其在 21 世纪的经济竞争力。在学校，数学和科学必须成为首选学科。美国应发起一项 K-12 学期的网络安全教育计划，以便进行数字安全、道德和保护教育；要扩展大学课程；要为在数字时代培养一支称职的人才队伍创造条件。正如总统曾提到的：“让我们的孩子为全球经济竞争做好准备，也基本没有比这个更为迫切的挑战了。”<sup>①</sup>为了完成这些目标，国家应该：

- 提高全民的网络安全风险意识<sup>②</sup>；
- 建立一个教育体系，以促进对网络安全的了解，并让美国继续在信息技术的科学、工程和市场领域保持和扩大领先地位；
- 为保护国家竞争优势，扩展并培训人才队伍；
- 帮助各类组织和个人在风险管理上做出明智的选择。

### 提高公众意识

形成对网上活动风险以及如何对其进行管理的广泛的公众意识，需要制定一个有效的战略。联邦政府应该与教育者及产业界部门一起，引导国家网络安全的公共意识和教育<sup>③</sup>。总统网络安全政策官应该负责这一公众意识战略的制定并指导其执行，并且应寻求国会、联邦政府、地方与部落政府、私营部门及公民自由与隐私组织的支持。这一战略应包括针对威胁开展的公共教育，以及有关如何加强数字安全、道德和安全。恶意行为者往往利用人们从互联网上接受信息或提供个人信息的意愿。这一运动应把重点放在通过公共信息来促进对互联网的负责任的使用，以及提高对欺诈、身份盗窃、网络侵略者和网络道德的意识。以往成功的公众安全运动，如对消防安全的“吸烟熊”以及对安全带的“点击和票务”运动可被用作向公众提醒网络安全重要性的一种模式。这些公共服务宣传活动的重点应使儿童和年龄较大的就业学生对网络安全熟悉。名人效应、随技术发展而成长起来的新一代以及新型媒体都可以在有效传播信息方面发挥关键作用。

### 提高网络安全教育

像第一颗人造卫星在 1957 年 10 月发射后的一段时期一样，美国处在一种取决于数学和科

---

① [www.whitehouse.gov/agenda/education](http://www.whitehouse.gov/agenda/education)，《教育》，2009 年 4 月 2 日，第 1 页。

② 跨部门网络安全工作组对 60 天评估有关问题的回应，2009 年 3 月 16 日，第 4 页；针对国家安全、网络战略向企业执行官的咨询函，2008 年 12 月，第 8 页。

③ 马里兰大学教育学院 2008 年研究报告，2008 年 10 月，第 4 节第 45 页。

学技能的全球竞赛中。据《经济学家》报告称，合格的信息技术雇员“在任何地方都是供不应求，但这种情况仍将继续严重化，因为所需的技能正在不断变化。除了技术知识，明天的 IT 雇员还将需要项目管理、变更管理、业务分析等专门知识。”研究报告指出，美国仍将继续拥有世界上最积极的 IT 企业环境，而且在提高企业竞争力的关键领域，包括教育、基础设施、鼓励创新以及法律等方面，有着更好的规模和质量<sup>①</sup>。然而，2007—2008 年度开展的计算学位和招生的 Taulbee 调查结果显示，美国的计算机科学与工程学士学位获得者的数目在下降，只有 2004 年的一半<sup>②</sup>。我们的国家无法容忍这一趋势继续下去<sup>③</sup>。

在所有部、局的参与下，美国政府应更多地支持关键教育项目以及研发项目，以确保国家在信息时代经济中的持续竞争力。现有的教育项目应得到评价以及可能的扩展，其他的活动可以作为项目扩展的模型，例如：

- 美国国家科学基金会（NSF）在 2006 年开始在“本科计算机教育振兴之路”中征求建议。这一项目旨在培养“美国的人才队伍，使其具备为民族健康、安全和 21 世纪的繁荣所必需的竞争能力和技能”<sup>④</sup>。
- 奖学金项目不仅为鼓励学生寻求网络安全教育，而且为其到联邦政府任职提供了激励。美国国家科学基金会和美国国土安全部在 34 个学院支持了奖学金服务项目<sup>⑤</sup>。在项目的前 8 年，有 1 000 多名学生获得了支持，80%的人最后到联邦政府工作。NSF 强调，鉴于扩大人才队伍的迫切需求，不能过分夸大研究和教育之间的协同<sup>⑥</sup>。
- 由国家安全局于 1988 年成立，并由国土安全部自 2004 年起协办的全国信息保障教育和研究卓越中心项目，在 38 个州及哥伦比亚特区的 94 个学院中推动了信息保障教育的提升，这些中心还与一些最有名的机构建立了合作关系<sup>⑦</sup>。美国国防部还在这些学院中赞助了信息保障奖学金项目。
- 全国高校网络国防防御竞赛，美国数学协会的数学奥林匹克竞赛，美国能源部“科学碗”，和西门子基金会的数学、科学和技术竞赛都提供了以竞争为导向的模式。美国国家科学基金会组织的一些学术界人士还引用了“DARPA 巨大挑战”项目、马尔科姆鲍德里奇国家质量奖以及高级加密标准竞赛等其他模式<sup>⑧</sup>。

### 扩大联邦信息技术人才队伍

总统的网络安全政策官，应通过与 ICI-IPC 的协调，考虑如何更好地吸引网络安全专业人士以及在联邦服务中保留住这些具有专业知识的员工。各部、局在从产业界吸引新员工方面已经取得了成功，但实施、转移或更新安全许可证所需的时间却在导致很多吸引人才的机会失去

① 经济学家情报处，《比赛、测试 IT 产业竞争力的手段》，2007 年 7 月，第 3 页。

② Stuart ZWen，《计算机学位和就业趋势》，2008 年 Taulbee 调查，第 4 页。

③ 21 世纪经济繁荣委员会，《在引才风暴中升起：为了更光辉的经济前景，赋予美国力量》，国家学术出版社，2007 年。

④ [www.nsf.gov/news/news\\_summ.jsp?cntn\\_id=109691](http://www.nsf.gov/news/news_summ.jsp?cntn_id=109691)。

⑤ 美国人事管理局 [www.sfs.opm.gov](http://www.sfs.opm.gov)，《联邦网络服务：服务奖学金》。

⑥ NSF，《对梅丽莎女士在国家科学基金会上所提有关问题的回应》，2009 年 3 月 31 日，第 1 页。

⑦ [www.nsa.gov/ia/academic\\_outreach/nat\\_cae/institutions.shtml](http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml)。

⑧ 见“supra”笔记，第 45 页。

了。联邦雇员必须能够建立起新的职业方式，他们可能不会在单一的机构内做事。共同的训练以及在各个机构间轮换任务，甚至可能在私营部门中轮换任务不仅是有效的，而且还将有利于相互交流和建立专业网络。

### 提高领导层的网络安全责任

美国政府应该继续在所有各级政府和工业界推动有关威胁、脆弱性以及有效实践方法的信息共享。只有工作人员理解网络安全的重要性是不够的，各级政府和工业界的领导必须能够把风险和及其潜在影响作为商业和投资决策的基础。州、地方和部落政府也面临着类似的问题。州政府经常作为创新的孵化器，其需要提供在管理信息和通信基础设施方面取得的经验教训。联邦政府应该继续与业界合作，以确定和传播在安全设计和运行信息技术产品方面的有效做法。

## 3. 共同承担网络安全责任

联邦政府如果闭门造车，那么其在保护网络空间的很多方面都不会成功。公共部门和私营部门的利益是交织在一起，它们有着确保安全、可靠的基础设施的共同责任，因为企业和政府的服务都要依赖于基础设施。不论在国内还是国际上，政府和行业领导者都需要划定角色和职责、整合能力以及负责发展全面的解决方案。只有通过这种伙伴关系，美国才能够加强网络安全并从数字革命中充分获益。网络空间安全的全球性挑战需要多边论坛的共同努力。在于私营部门的持续合作下，这种努力应致力于提高互操作网络的安全，方法是制定全球标准，扩大以法律体系打击网络犯罪的能力，继续开发和推广最佳做法，并保持稳定和有效的互联网治理。

### 改进私营部门和政府的关系

美国政府有责任保护和捍卫国家的安全，各级政府也有责任确保其公民的安全和福祉。然而，私营部门设计、建造、拥有和经营着大部分的网络基础设施，这些基础设施同时支持了政府和私人用户。工业界和政府应该共同对基础设施及其上的交易的安全和可靠性承担责任。它们应密切合作，解决这些互依赖问题。联邦政府可以采取很多方法来应对这些挑战，其中一些可能需要修改法律和政策。

私营部门需要参与其中，以帮助解决执法和国家安全中的一些局限性。现行法律允许使用一些工具来保护政府而不是私人网络，反之亦然。行业领导者可以开展企业的信息共享，从而为政府提供帮助，但其还要为企业风险、数据破坏的底线影响、企业间谍活动以及服务丧失或退化负责。行业领导者可以要求更高的保证，这些保证来自于供应商和服务供应商的要求，因为他们有责任创造更安全的软件和设备。企业需要有效的手段来在彼此之间或者与政府共享检测方法，以及关于安全事件和攻击方法的信息、修补技术以及取证能力。

如果风险和后果可以货币价值来衡量，那么各个组织将有更大的能力和动力来解决网络安全问题。特别是，私营部门往往要求有商业案例来证明其对信息和通信系统安全的资源支出是合理和正确的。政府可以考虑基于激励的立法或管理工具来提高价值主张，并为促进和提高合作关系和信息共享而创造环境<sup>①</sup>。

---

<sup>①</sup> 微软公司 Scott Charney 在众议院国土安全委员会新威胁、网络安全和科技子委员会上的证词，2009 年 3 月 10 日，第 4～5 页；战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 49 页；互联网安全联盟《行为准则——哈萨维的问题》，2009 年 3 月 24 日，第 2 页，第 4～7 页。

总统的网络安全政策官应与相关部、局以及私营部门合作来审查现有的公共-私营合作关系以及信息共享机制，以寻找或建立最有效的模式。在过去的 10 年间，作为美国关键基础设施保护和网络安全政策的基础，公共-私营合作关系促进了信息共享和服务。在这段时间内，联邦政府和私营部门参与了若干关于网络安全及信息和通信基础设施相关问题的论坛<sup>①</sup>。

这些团体开展了很多可贵的工作，但工作的分散也使一些参与者有挫败感，认为角色和责任模糊、能力不均衡以及各种计划和建议激增。政府和私营部门的人员、时间和资源在众多机构中呈分散的状态，从事着重复或不一致的工作。公共-私营合作关系的发展必须明确界定这种合作关系的性质、各个团体的角色和责任、对各方贡献的期望以及机制。联邦政府应合理化和聚合其资源，并向现有的组织提供，以优化其确定优先级的能力，以便更有效地开展工作和制定响应与恢复计划。

60 天的审查过程中，审议了一些有效的公共-私营合作模型<sup>②</sup>。虽然这些模型的功能各不相同，但它们有一些重要属性却是一样的，都有着一个明确界定的使命，参与者的角色和责任也得到了明确定义，并有清晰的价值主张，这些价值主张为参与者创造了激励因素。每个模式都在参与者间建立了信任环境，减轻了参与者的忧虑。现有的网络安全合作关系也可能需要使用这些模型的最有效的特点。

### 评估影响公共-私营合作关系的潜在障碍

一些私营部门的成员继续表示了对某些联邦法律可能阻碍全面合作关系以及信息共享的关注。例如，一些业界人士认为，在这种合作关系下，同一行业中一些合作者的信息共享和集体规划可以被认为是“合谋”，或者违反禁止对贸易进行限制的法律<sup>③</sup>。业界还对向联邦政府披露敏感或专属商业信息，如脆弱性以及数据或网络破坏情况表达了保留意见。尽管贸易保护法和关键基础设施保护法为这些信息提供了保护，目的就是解决信息自由法所带来的问题，但业界的这种关注仍没有消减。除此之外，业界也担心信息共享所带来的名誉损害、法律责任或监管后果。相反，联邦政府有时却限制了与私营部门共享政府的信息，因为它们需要保护敏感的情报来源和方法，或者是因为隐私原因。

这些问题并不是孤立存在的。反托拉斯法为防止不公平竞争提供了重要的保障措施，信息自由法有助于确保政府的透明度，这对维持公众的信心是非常重要的。公民自由和隐私团体认为，将保护范围扩大只会使人们获得逃避责任的法律借口。此外，考虑到更加复杂的全球信息和通信市场的特性，信息共享问题将会进一步复杂化。当在美国的成员企业为外商独资时，强制性信息共享，或者将这些公司从信息共享制度中排除，都可能是贸易问题。

作为合作关系中的一方，政府应与私营部门创造性地开展工作和合作，以确定合适的解决方案，既考虑到交流信息和保护公共利益与私人利益的需要，还要采取综合办法以保护国家和经济安全。这些解决方案应确定明确的、可操作的数据共享目标，并界定事件报告标准。如果

① 这些组织包括：关键基础设施合作咨询委员会（CIPAC）及作为这一体系组成机构的可持续性安全框架工作组、部门协调委员会（SCC）、政府协调委员会（GCC）；联邦调查局的 InfraGard；美国特勤局的电子犯罪特别任务组；国家安全电信咨询委员会（NSTAC）；国家基础设施咨询委员会（NIAC）；国土安全咨询委员会；其他相关的子委员会和工作组。

② 包括国家网络取证和培训联盟、跨部门网络安全工作组（CSCSWG）以及英国的一些咨询模型。

③ 如《Sherman 反托拉斯法》（《美国法典》第 15 编，2004 年）。

能有不需要数据所有权易手的解决方案，私营部门将更加乐意，如在英国模式中，使用经审查的信息安全供应商进行数据整合，而不是由政府去做。

最后，联邦政府应该使学术界、公民自由和隐私团体、开放政府的倡导者、消费者参与进来，以确保政府的政策充分考虑到他们所代表的群体的广泛利益。离散的过程、政策或技术事项一般都会有很多问题解决不了。技术变革往往带来政策考虑，并有可能要求改变现有的过程。政策的改变（如通过法规或税收激励措施）可以影响到采购或技术研发。美国政府还可以考虑集中更多的资源用于“改变游戏规则”的研究领域，如基于行为、政策或激励的网络安全解决方案。这些问题的交织性质要求所有利益相关方的利益都得到表现。

### 与国际社会有效合作

对建立一个安全和繁荣的数字化基础设施而言，国际规范是至关重要的。美国需要制定一项战略来塑造国际环境，使志同道合的国家一起就一系列问题探讨，包括领土管辖权、主权责任、武力使用等问题的准则。此外，不同国家和地区的法律和惯例，如与网络犯罪调查和起诉、数据保存和隐私保护有关的法律<sup>①</sup>，有关网络防御和响应网络攻击的方法，对实现一个可靠、安全和强健的数字环境提出了严重的挑战。解决这些问题，需要美国与所有国家，包括那些在建立自己的数字化经济和基础设施时遇到同样问题的发展中国家，以及国际机构、军事盟友和情报合作者共同努力。

在过去 10 年中，美国的联邦通信、基础设施和网络安全有关政策制定是沿多条路径的。一个更加一体化的政策制定方法将使这些政策的目标相互强化，使美国有一致的、更有效的立场来利用其国际机会。美国应该采取一种综合的办法来在很多实质性领域间实现国家利益，包括网络安全、保护言论自由和其他的公民自由，以制定一致的政策。

总统的网络安全政策官应该与各部、局合作，加强和整合跨机构的政策制定过程和国际网络安全立场协调过程。此外，联邦政府将会继续其与私营部门合作的长期历史，应针对如何利用各个国际标准化组织制定一项主动参与计划。这将包括评估现有的政策，对国际立场的制定、完善或重申进行协调，以确保与网络安全有关的经济、国家安全、公共安全和隐私利益都得到了考虑<sup>②</sup>。10 多个国际组织，包括联合国、八国集团、北约、欧洲理事会、亚太经合组织论坛、美洲国家组织、联合国经济合作与发展组织、国际电联、国际标准化组织都在涉及与信息通信基础设施相关的问题<sup>③</sup>。还有一些新的组织已开始考虑网络安全有关的政策和活动，而另一些则在扩大其现有的工作范围。这些组织考虑的政策和开展的活动有时是冲突的，并且往往重叠。它们发布的协议、标准或做法会产生全球影响，不容忽视。数量之多、类型各异以及重点不同，限制了很多国家，包括美国的政府进行充分参与的能力。

总统的网络安全政策官应与各部、局合作，对采用何种国际平台制定网络安全相关网络安全协议、标准、活动和政策，进行标识、跟踪并排列优先级，且增强谈判、讨论能力。过去的经验表明，美国将有必要继续参与各种国际活动。联邦政府应加强与私营部门和其他国家的合作，以确保能全面参与到合适的论坛之中，处理未来的全球信息和通信基础设施发展中影响美

---

① 例如，欧洲网络犯罪公约委员会是为确保网络犯罪法律和执法工作的一致性开展的一项重要的国际努力。虽然美国和其他很多发达国家是这一约定的缔约国，但大多数国家还没有签署或批准。

② 战略与国际研究中心（CSIS）对第 44 任总统的网络安全建议，2008 年 12 月，第 11～13 页。



国利益的最重要的问题。美国及其盟国应该充分利用彼此参与地区性或其他论坛的机会，以推动共同的政策目标，并关注现有国际组织的工作，减少其中的重复性劳动。例如，国际电联和国际标准化组织都在制定网络安全取证相关标准。美国还应该寻找机会，以促进各类广泛的论坛中涉及的信息和通信基础设施的安全和发展。

在与私营部门的合作下，联邦政府应当协调和扩大国际伙伴关系，针对美国企业、政府服务、军事和国家所依赖的信息和通信基础设施，涵盖全面的网络安全相关活动、政策以及机遇。各国政府和工业界可能需要签订新的协议来促进国际信息共享以及战略和业务合作。美国政府应为推广和建立国外能力而增加资源和注意力。例如，美国应加速帮助其他国家建立法律框架和打击网络犯罪的能力，以及制定网络安全实践措施和标准的能力。美国也应与盟友一道，确保互联网稳定性和全球互操作性，提高其对所有用户的安全性和可靠性<sup>①</sup>。

#### 4. 建立有效的信息共享和事件响应框架

美国需要建立一个全面的框架，以便协调政府、私营部门和盟国共同应对重大的网络事故。联邦、州、地方及部落政府应与业界合作，完善其用于提前检测、预防及应对重大网络安全事件的计划和资源。由于此类事件可能影响到政府和产业界部门之间的互联网络，因而在重大事件发生之前、期间和之后，对此类计划和行动进行协调就显得特别重要。例如，尽管收到了提前预警和如何保护的指导，但当“Conficker”蠕虫病毒在2009年4月1日激活且带有恶意的附件时，仍有一些联邦部、局没有做好应对准备。

##### 建立事件响应框架

与其他重大国家事件一样，在发生重大网络事件时，只有白宫有权协调与事件响应相关的一系列职能部门和权力机构。各部、局应按白宫总体战略方向履行各自责任。总统的网络安全政策官应同时是白宫网络事件应急的行动官员（其职能与帮助白宫检测恐怖主义袭击或自然灾害的行动官类似）。

联邦政府应建立一套明确且具权威性的网络事件响应框架，并纳入修改后的《国家响应框架》的“网络事件附件”中。到目前为止，针对网络事件的联邦响应还未统一。对于涉及国家安全/应急通信的情况，第12472号美国总统令确定了今天的这些授权和处理流程。然而，根据当前的法律政策，各部、局仍各自负责决定和实施如何隔离、保护和恢复自身计算机网络和数据的措施。

在网络安全和其他联邦网络之间，由于法律现状而非人为差异，联邦网络事件响应的责任分散到了不同的联邦部、局之中。根据事件的性质，如重大的漏洞、犯罪袭击或军事事件，不同部、局可能

##### 网络运营商和服务提供商

互联网由管理其运行和为客户提供服务的企业联合运营。网络运营商负责建立和维护信息通信基础设施，为客户提供接入和宽带服务。服务提供商负责提供互联网接入网关、安全服务、存储或处理服务以及信息的获取（如互联网地址或新闻）和应用（如搜索引擎）。一个公司可以同时提供接入、信息和服务（如社交网络）。

<sup>①</sup> 美国商会《致国家安全委员会的信》，2009年3月27日，第3页。

负有或承担着主要的应急责任，而其他部门或机构则可能对此一无所知。另外，对整个事故的责任分配可能还不明确。尽管每个参与者都有着明确的专长领域和法律授权，但他们很难统一到一个单一的协调框架中。把任何权力部门合并到一个统一架构中可能都需要通过法律来实现。信息和通信基础设施跨部门政策委员会（ICI-IPC）的进程应明确事件响应相关的不同部、局的角色、职责及资源，鉴于事件响应涉及很多方面，涉及多个领域的不同力量，必要时要对这些角色、职责及资源协调或强化，要把网络安全、执法、情报及军事等部门拉到一起来讨论。

众多评论者都强调了建立事件报告和响应阈值的重要性。网络运营商和服务提供商每天都会处理大量尚未达到“滋扰”级别的事件。在这些低级别事故中，藏匿有相对少量的可能产生巨大影响的入侵或攻击。其他政府和私营部门的网络运营商很想了解此类事件的技术细节，以帮助其抵御相似的网络威胁；执法部门和情报机构也可借此跟踪并寻求有关方法来制止网络安全方面的犯罪和来自国外的威胁活动。

联邦政府应与州、地方和部落政府及业界合作，总结一系列威胁的场景和衡量指标，以供风险管理决策、制定恢复计划及确定研发优先顺序。同时应发展建模和模拟能力，以有助于演练这些计划并确定可能的破坏级别。

信息和通信基础设施跨部门政策委员会（ICI-IPC）应在各部、局中建立明晰、可执行的事件即时报告规则，以便提高机构间响应的效率。对于在各自管辖范围外的事件的报告，各部、局存在差异。如能即时报告横跨各部、局的重大事件，则将有助于形成联邦的整体应急响应能力。

总统的网络安全政策官应与信息和通信基础设施跨部门政策委员会（ICI-IPC）合作，确定发展和保持态势感知及事件响应能力的最有效方法。《国家网络安全综合计划》应继续致力于提高联邦网络的防御能力，同时考虑调整实施计划或增添内容的需要。总统的网络安全政策官尤其应该：

- 与私营部门合作，探索如何更好地将技术能力应用到国家基础设施的防御中来，以及需要什么样的法律框架来保障隐私权和公民自由。
- 审议国家网络安全中心（NCSC）的运行理念及其实施情况，研判该中心关于责任、资源战略和管理的提议是否充分，使其能够提供支持网络事件响应工作所必需的态势感知共享信息。
- 继续向可信互联网接入项目的目标迈进，减少政府网络接入的数量，同时基于对现实挑战的评估，再次考虑项目中的目标和时间表。在过去的两年中，一些部、局在减少互联网接入点数量和部署系统上取得了进步，这些系统将有助于联邦政府阻止并检测恶意的行为。然而，政府在充分发挥能力之前仍然有很多工作要做，而且可能需要考虑进一步的政策以促进战略的全面实施。
- 要与公民自由和隐私团体继续协商，评估并在必要时继续实施联邦入侵检测和防御系统的试点部署工作，考查这些系统的性能，并且继续研究若将这些系统应用到州政府系统中会产生的问题。这些传感器将对联邦网络获得态势感知信息具有关键作用。随着这些部署工作的进行，政府也将从中获取很多政策、法律或技术层面的经验教训。
- 与业界、公民自由和隐私团体协作，探讨其他长期性的入侵检测和防御体系结构。

联邦政府应提高其向总统提供网络入侵或攻击的战略预警的能力。联邦政府应继续将国家的长期投资项目投向基础性的密码、信息保障技术和其他必要的基础设施。这些投资以及其他的情报能力，对于网络攻击的战略预警至关重要。此外，针对保护国家关键基础设施的需求，

联邦政府应找出执法能力或投资权限上的不足。任何新的授权需始终与保障公民自由和隐私权相一致。

美国政府应对有助于防御网络应急事件的流程、技术和基础设施进行投资。可选项包括提升安全测试能力，或投资于自动化或集中化的网络管理系统，以及对某些非涉密系统实施更严格的互联网接入。

政府需要建立一套可靠持续的机制，以便将所有相关信息整合在一起，形成一张共同的运行图。联邦网络安全中心之间经常分享彼此的信息，但其中没有一家机构可以将来自不同中心和其他资源处的所有信息综合起来，制成一张不断更新且涵盖网络威胁和网络状况的全局图，以预报迫在眉睫的应急事故，以及支持协调事件响应。国防部负责整合关于网络健康和状况、入侵企图和对自身网络的攻击的信息；情报界负责自身网络；US-CERT 负责民事联邦机构以及在某种程度上对私营部门负责；执法和情报机构收集与网络有关的犯罪和国外威胁活动证据，当然也需要具有处理有大规模犯罪活动的的能力。

联邦政府应考虑若信息和通信基础设施遭受重大损害，尤其是当信息和通信网络融为一体时，是否有充足的可用替代品或通信设施储备。基础设施的替换或修复也要求有额外的计划和资源，尤其是当网络或电网中难以替换的元件受到物理损害时。

联邦政府应利用现有资源，在各级政府和私营部门间建立有助于防御、检测和应对网络应急事件的流程。联邦政府应利用州际信息共享和分析中心、全国 58 座州立和地方融合中心等现有资源，帮助建立信息和通信基础设施方面的态势感知能力。

#### 加强信息共享，提高事件响应能力

信息是防御、检测和应对网络事件的关键。网络软硬件提供商、网络运营商、数据所有者、安全服务提供商以及某些情况下的执法或情报机构可能各自拥有信息。这些信息能够帮助检测和了解复杂的入侵或攻击问题。只有将上述各类信息源整合起来，才有可能全面了解事件并做出有效的响应，使所有人受益。

联邦政府应与州、地方和部落政府及私营部门，包括数据所有者、网络运营商及隐私和公民自由专家合作，寻求网络安全方面的信息共享方案，消除对有关隐私和专属信息的担忧，使信息共享符合国家的利益，达到互利的目的。私营企业关心其信息的潜在使用问题，政府必须保障其隐私权，公正执法，保护情报来源和方法，以及保护可能导致不公平竞争优势的政府信息。为了解决这些担忧，政府和私营部门都需要做到透明、诚信。可选方案包括：

- 设立一个政府和私营部门都信任的第三方非营利性、非政府组织，作为政府和私营部门共享信息的平台，以此提高政府和私营部门的关键网络的安全性。此类组织可使用商业服务，并且不会扰乱日益壮大的安全服务市场。
- 联邦政府（如执法机构）与个体公司或公司集团，可能还有州、地方和部落政府的参与，持续接触，在特定的部门或区域内实现一定程度自愿性的信息共享，而不是在更广泛的背景下共享信息。

美国政府应与受影响方和国会协商，考虑制定经裁剪的信息共享激励措施。作为最后的手段，这些措施可以包括监管措施，以满足社会对强健、韧性的关键基础设施，以及公民自由和隐私权保护，并维护作为美国经济系统基础的公正、公开的经济市场的需求。加密或受控访问认证等隐私增强技术可减少信息共享中的某些风险。

联邦政府应全面评估妨碍网络安全信息共享的有关安全分级和人员涉密等方面的政策，同时寻求信息共享改善方案，并确保公民自由和隐私权得到保障，敏感信息得到适宜的保护。联邦政府各部、局当前关于信息搜集，使用、保留和传播的政策很大程度上都是基于法定权限、对隐私和公民自由的关注、对来源和方法的担心以及历史惯例而来。这些政策严重阻碍了联邦政府间的网络安全信息共享。在评估安全和适用性进程的相关工作时，应将联邦政府通过“安全性和适用性改革倡议”所取得的进展以及“信息共享环境”相关工作考虑在内。

联邦政府应与私营部门合作，制定私营部门网络运营商向联邦政府进行事件报告的标准。业界表达了作为受害者对报告其网络事件的担心，包括随之而来的股东的担忧、市场反应或监管行动所带来的潜在消极影响<sup>①</sup>。一家产业界的组织提议成立政府-企业工作组，设立具体到各个关键基础设施部门的网络事件阈值，以保证将信息报告给安全官员<sup>②</sup>。需制定相应的规则并监督政府对此类信息的使用，以保障隐私权和公民自由。另一完善报告程序的途径是考虑适当的数据泄露通知法案，要求企业将相关信息通知给公众和政府，其中包括可进行调查的执法部门。联邦政府也应检查已有的市场监管汇报规定的有效性和工作范围。与此同时，联邦政府需制定与私营部门进行事件报告共享的流程和规则。这些规则的制定需考虑密级和隐私问题。另外，联邦政府应协助研究界获得网络安全事件数据，并对此加以适当控制，以便于开发工具、测试理论和制定可行的解决方案。此类共享需要解决关于敏感或专属数据及个人身份信息的保护问题。

联邦政府应努力扩大与主要盟友在网络事件和脆弱性方面的信息共享，寻求改善网络安全的双边或多边安排，并确保这些安排符合美国其他方面的经济和安全利益，使公民自由和隐私权得到保障。国际合作为美国政府与私营部门的合作带来了更多挑战。若美国政府计划与其他国家共享美国私营企业的行业信息，则国内守法的私营部门关于信息共享的担忧将会增加。需要再次指出，私营部门向政府共享的信息的控制、传播和使用应得到明确说明并可追责，包括如何管理美国和国际社会之间对共享信息的使用。

### 提高所有基础设施的网络安全

在私人拥有的关键基础设施和重要资源的防御工作中，联邦政府应与私营部门合作，明确公共-私营关系的角色和职责。联邦政府的核心责任之一即是共同保护私营关键基础设施不受武装攻击、物理入侵或国外军事力量、国际恐怖分子的破坏。同样，政府也在保护这些基础设施不受罪犯或国内恐怖分子的破坏上发挥着重要作用。然而，若攻击是通过计算机网络远程进行而非直接的物理行为，那么政府应对相同的行为体攻击相同基础设施且造成相同损害的情况负多大程度的责任，这个问题尚未解决。大多数网络运营商和服务提供商都将自身网络的维护和防御工作归为自己的责任，但私营部门的很多重要组织已表示，业界希望形成一个工作框架，在此框架下政府将追捕恶意为人，为私营部门运营商提供信息和技术支持，帮助私营部门保护自身网络<sup>③</sup>。

---

① TechAmerica 对 60 天评估的回应，2009 年 3 月 21 日。

② 跨部门网络安全工作组（CSCSWG）对 60 天评估有关问题的回应，2009 年 3 月 16 日，第 11~12 页。

③ CSCSWG 对 60 天评估相关问题的回应，2009 年 3 月 21 日，第 1~2 页。NSTAC 对 60 天评估工作组的回应，2009 年 3 月 12 日，第 3~4 页。信息技术和通信领域的部门协调委员会对白宫 60 天评估相关问题的回应，2009 年 3 月 20 日。

在网络安全解决方案的制定过程中，联邦政府应考虑出台鼓励集体行动和竞争的激励措施。例如，网络空间至今还未出现“保护性标准”的法律概念。可能的激励措施包括调整法律责任（安全改善后可以减责，安全条件变糟糕则导致责任增加）、补充赔偿、税收鼓励政策以及新的监管规定和执行机制。

总统的网络安全政策官应与各级政府、私营部门及国际伙伴合作，制定有关战略和计划，鼓励创新型网络安全解决方案，确保基础设施系统的安全和韧性。基础设施的案例包括：

- 政府应协助世界银行、国际货币基金组织等国际金融机构，向其提供必要的信息、工具及专业知识，并鼓励其运用最佳实践措施来保护自身的信息系统。这些组织的系统曾在 2008 年遭受一系列严重入侵<sup>①</sup>。
- 《美国复苏与再投资法》通过储备基金来推广医疗信息技术的使用。随着电子记录保存技术在互联网上变得日益普及和获得，病人信息的保护工作是否能得到公众认可，这将十分关键。
- 能源部应与联邦能源监管委员会合作，决定是否需要为能源方面的工业控制系统另行制定安全强制要求和程序。另外，随着新的智能网技术在美国的普及，联邦政府务必要制定和通过相应的安全标准，以避免使对手获得新的机会侵入上述系统或对其发动大规模攻击。
- 交通部下属的美国联邦航空管理局在维持现有系统的同时，已制定了向下一代空中交通控制系统过渡的长期计划。交通部检察长于 2009 年 3 月 18 日在众议院航空交通和基础设施子委员会上作证时称，需要评估潜在的安全脆弱性，制定一套健全的网络安全战略和设计方案<sup>②</sup>。

## 5. 鼓励创新

信息和通信部门正在创建一个融合平台，使数据、音频和视频共享共同的基础设施。当前国际互联网模型的非中心化性质，可以使个人和企业家在无须得到许可的情况下，开发并配置创新的应用程序。创新带动了价值数十亿美元的新型业务，彻底改变了用户与网络及用户彼此之间的互动方式。随着科技对美国越来越重要，对于这一不断演变发展的基础设施，保持信心和信任至关重要。总统已呼吁联邦政府同业界保持合作，共同开发“下一代的安全计算机和应用于国家安全的网络互联”，制定“新的、严格的网络安全与物理韧性新标准”，以及

### 对于韧性的要求

面对物理破坏、非法操作和电子攻击，基础设施必须具有一定的恢复能力。除了保护信息本身，网络空间风险减缓战略必须关注用于访问基础设施的设备、支撑性的网络组件，以及所有用于移动、存储和处理信息的手段。这一战略还必须包括对威胁的预防、减缓和响应，保护运营人员、基础设施的用户、基础设施的处理进程以及用于建设和运维基础设施的供应链。

① [www.foxnews.com/story/0,2933,435681,00.html](http://www.foxnews.com/story/0,2933,435681,00.html)，《史无前例的危机》中的“网络攻击下的世界银行”，2008 年 10 月 10 日；[www.foxnews.com/story/0,2933,452348,00.html](http://www.foxnews.com/story/0,2933,452348,00.html)，《网络黑客侵入 IMF 计算机系统》，2008 年 11 月 14 日。

② [www.oig.dot.gov/item.jsp?id=2442](http://www.oig.dot.gov/item.jsp?id=2442)，交通部检察长在众议院航空交通和基础设施小组委员会上的证词，2009 年 3 月 18 日，第 7 页。

“保护个人数据的标准”<sup>①</sup>。

美国应充分利用技术创新，以消除网络安全的担忧。虽然市场上早就存在着很多可以明显增强安全性的技术和网络管理的解决方案，但由于成本或复杂的原因，这些技术和解决方案并没有得到广泛应用。另外，鉴于国际互联网基础设施的内在设计，现有的解决方案已发挥到了极限，无法再继续提高。从长远来看，开放和创新将有助于建立一个透明且责任明晰的更加强大的基础设施。联邦政策必须满足国家安全要求，保护知识产权，并且要保持基础设施的可用性和连续性，即便在其遭受复杂对手攻击的情况下。联邦政府还必须注意不要制定一些不必要的政策与规章，它们可能会妨碍创新、导致低效率或使安全性降低。

## 未来

根据 2006 年的国家研究院报告《振兴美国的通信研究》一文指出：“通信网络是庞大、复杂的系统，其可靠性、安全性及演化性取决于连贯的、被广为接受的体系结构概念的发展<sup>②</sup>。”这一报告还指出：“有多家厂商的产品被用来配置美国的电信基础设施并提供服务……它们跨越了供应商的边界。由于业界正转向水平化的结构，并分解出了大量的小型公司，不论是厂商还是服务提供商都不会准备去负责端到端系统的设计。”

这样一来，就没有统一、整体的视野去指导私营部门、学术界和政府政策、标准、研究、市场开发或采购做出决策。联邦政府、私营部门及其他利益相关方应为未来基础设施共同制定技术中立的性能和安全目标，既满足其作为消费者的自身需求，同时又发挥其作为公众利益管理人的作用。联邦政府同其合作伙伴应针对具体的关键基础设施部门和组织，分别制定一个经协调的国家信息和通信基础设施目标族。这些目标可以参考不同的计算平台模型或网络控制概念，以及通过政府、学术界或业界的研究项目产生的技术解决方案。

数据和服务向第三方的联网服务器的移动被称作“云”，这为全球的私营部门和政府带来了新的政策挑战。跨越司法管辖边界的数据移动带来了执法挑战，也对不同国家开展的隐私与公民自由保护带来了挑战，数据或网络出现泄露事件时的决策责任也不好确定。有些客户会试图限制服务提供商移动或存储数据的地点，而另一些跨国经营的客户则会寻求利用地理和时区的差异带来的好处。

## 基础设施安全愿景

有很多工作都定义了某些技术或基础设施的愿景。例如，美国能源部与业界合作，于 2005 年推出了一个为期 10 年的路线图，以保护电网中的控制系统（[www.controlsroadmap.net](http://www.controlsroadmap.net)）。这项工作的愿景是，截至 2015 年，“关键应用的控制系统的设计、安装、运行和维护能够承受蓄意的网络攻击，不会丧失关键功能”。国防部高级研究计划局（DARPA）的顾问小组把对当前基于 IP 的网络的保护看作是没有前途的，呼吁“对可替换的体系结构进行独立的考查”，以便测试和评估最佳候选方案。根据 2009 年 3 月的一份简报，国防部高级研究计划局正在进行一项为期 6 个月的候选方案分析。

① [www.whitehouse.gov/agenda/homeland\\_security/#protect-our-information-networks](http://www.whitehouse.gov/agenda/homeland_security/#protect-our-information-networks)，国土安全进程《保护我们的信息网络》。

② [http://sites.nationalacademies.org/cstb/CompletedProjects/CSTB\\_042246](http://sites.nationalacademies.org/cstb/CompletedProjects/CSTB_042246)，《振兴美国的通信研究》，2006 年，第 36～37 页。

### 将研发框架与基础设施发展联系在一起

在总统网络安全政策官的领导下，联邦政府应与其他总统行政办公室及信息和通信基础设施跨部门政策委员会（ICI-IPC）进行合作，在现有的网络和 IT 研发（NITRD）战略及其他相关研发工作的基础上，针对可以满足基础设施目标的、改变游戏规则的技术，制定研发战略。联邦政府应扩大这些战略同业界与学术研究工作的协调，以避免重复性的工作，充分利用具有互补性的有关功能和议事日程并保持同步，并且确保能实现技术转移及进入市场。

- 为了提高美国的竞争力，联邦政府应与业界合作，包括鼓励学术界与业界实验室之间的协作，共同制定迁移路径和激励措施，以快速采用研发成果。
- 联邦政府还应与私营部门及其他利益相关方合作，利用基础设施目标和研发框架来确定国家标准化工作及参与国际标准化组织有关工作的目标。

### 将身份管理作为选项

如果不能提高身份鉴别水平，我们就无法提高网络安全性。身份管理不只是用于人员认证。鉴别机制还可以帮助确保在线交易使用的只是对于网络和设备而言可以信任的数据、硬件和软件。对大多数互联网交易而言，在如今的系统中，与人们建立信任关系所用的东西类似的电子化的技术等也许还匮乏、不完整或者难于理解和实施<sup>①</sup>。基于不同程度的身份公开和彼此约定的责任制，身份管理能够为组织和人员建立可信的社区，同时排除不受欢迎的入侵者或不合适的成员请求。身份管理通过对个人可识别信息的传播进行进一步的保护，还可能提高隐私水平。

联邦政府在与业界及公民自由与隐私社团的合作下，应共同制定一个基于网络安全的国家身份管理愿景与战略，为此需要考查一系列方法，包括隐私增强技术。联邦政府必须通过大量的资讯、服务与福利项目同公民展开互动，政府要对保护公众的隐私信息产生兴趣。在线交易变得日益普遍，涉及金融、卫生与商业等诸多方面，需要一个在交易方之间建立信任的基础。

- 对于具有高度价值的业务（如智能电网），国家应建立一系列可以选择加入（opt-in）的、互操作的身份管理系统，以便为在线交易建立信任并提高隐私水平。
- 国家科技委员会（NSTC）下设的生物测定和身份管理子委员会于 2008 年发布了一项报告，提供了对未来联邦身份管理的愿景以及一系列的研发建议<sup>②</sup>。联邦政府应把这项报告作为身份管理战略的出发点。
- 联邦政府应与国际伙伴进行合作，共同制定相关的政策，鼓励发展可信的全球生态体系，以保护隐私权和公民自由，并对如何适宜地通过执法活动保护公民和基础设施给出说法。

遵循第 12 号国土安全总统令，联邦政府正努力在整个联邦范围内充分实施联邦的互操作性身份证书机制。联邦政府应为全面落实第 12 号总统令提供相关的资源。联邦政府还应考虑将联邦身份管理系统扩展到关键基础设施的运营商，以及私营部门的应急响应和修复服务提供商，以便于在国家应急状态下使用。

<sup>①</sup> [www.microsoft.com/mscorp/twc/endoendtrust/vision.aspx](http://www.microsoft.com/mscorp/twc/endoendtrust/vision.aspx), Scott Charney, 《建立端到端的信任》，微软公司，2008 年，第 5 页。

<sup>②</sup> [www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf](http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf), 总统行政办公室的国家科技委员会给出的身份管理任务组报告，2008 年 7 月。

## 全球化政策与供应链的整合

信息技术革命及自由贸易政策的结果之一，是信息和通信技术产品的全球化的研究、设计、制造与服务环境，这些产品由在全球范围内分布分支机构的企业所提供。这一全球市场通过美国的高科技商品和服务打开了世界范围内的市场，给美国创造了巨大的利益。然而，新的制造、设计与研究中心在全球范围内的出现，使人们更加担忧微小的硬件或软件操作会更加轻易地导致计算机和网络的崩溃。仿造产品已带来了最明显的供应问题，但记录在案的明确、蓄意的破坏的例子却很少被公之于众。

我们需要的是广泛、全面的风险管理，而不是一味地否定外国产品与服务。供应链攻击所面临的挑战是，老练的对手也许会专门盯着特定的系统，所实施的篡改几乎让人无法察觉。国外制造的确会给国家级对手带来了更加容易破坏产品的机会，但是，通过招募关键内部人员或通过其他的间谍活动，也可以实现同样的目标。

最好的防御也许是通过持续的创新来保证美国的市场领导地位，并且维持一个多样化、韧性的供应链和基础设施。通过与各部、局合作，总统网络安全政策官应：

- 以国家安全局为国防部所做的工作为基础，通过总务管理局（GSA）制定商业产品与服务的采购战略，以便建立市场激励机制，使安全成为硬件与软件产品设计、新的安全技术及安全管理服务的一部分。
- 扩大同州、地方与部落政府及国际合作伙伴的合作，以便使这些采购的市场影响最大化。
- 同国会一起明确相关的机制，使各部、局在适当的特定情形下，在做出购买决定时考虑相关的威胁信息。
- 从经济和威胁的角度出发，与业界合作提供威胁信息并确认管理供应链和内部风险的最佳方案。

## 保持国家安全/应急战备能力

联邦政府保护美国民众和提供共同防御的义务包括负责确保国家在危机时刻能够进行通信并做出响应。通信系统可能会最先遭受此类事件的冲击，因此必须具有可以恢复的韧性或能力，以便管理事件响应活动并保护政府的职能。《1934 年通信法》授权总统在处于从“公共危险状态”到“战争”的各种条件下时，如果其认为有必要维护国家安全、国防并且存在必需的阈值条件的话，可以使用、控制或者关闭联邦通信委员会管辖下的通信服务、系统和网络。第 12472 号行政令要求建立一个政府和业界联合的国家协调中心，以在所有的危机或应急条件下，为通信服务或设施的启动、协调、恢复或重建提供帮助。第 51 号国家安全总统令/第 20 号国土安全总统令《国家连续性政策》（2007 年 5 月 4 日）在联邦政府内对有关连续性通信的角色进行了分配。

国土安全部正在努力朝着这一目标前进：向国家安全和紧急系统用户提供下一代网络的融合信息服务，并确保在各种灾难及其他会致使公众用户遭受通信服务严重恶化或中断的事件期间，其所提供的服务具有极大成功的可能性。下一代网络在国家安全方面的改进将包括数据、音频与视频等多种服务。由于主要运营商和服务提供商所构想的体系结构具有较大差异，这会使得国土安全部的努力变得复杂化。为此，国土安全部正在考查、比较不同的方案，并争取在提交给标准化组织进行考查的方案上与业界达成一致。联邦政府应：



- 针对下一代网络的国家安全与应急战略通信的能力，制定一个协调计划，包括进度与经费开支要求。
- 提供其他的附加服务选项，使联邦政府可以获得，或者引导政府将用在信息和通信基础设施上的投资用于增强在自然灾害、危机或冲突时期的通信设施的存活性。
- 与国际合作伙伴与标准化组织进行配合，以便在遍布全球范围内的下一代网络环境中维护下一代国家安全/应急战备通信能力。
- 确保与制定行政部门连续性通信体系结构有关的工作，以及下一代服务项目都获得了充足的人力资源支持。

## 6. 行动计划

评估小组建议了如下的近期和中期行动计划。

### 近期行动建议

(1) 任命一名网络安全政策官，负责协调全国的网络安全政策和活动；建立一个强大的国家安全委员会的网络安全指挥部，受网络安全政策官的指导，并向国家安全委员会和国家经济委员会报告，以协调部门间对网络安全有关战略和政策的制定。

(2) 为总统起草新版的保护信息和通信基础设施的国家战略，这一战略应包括对 CNCI 活动的持续评估，必要时延续 CNCI 已经取得的成功。

(3) 将网络安全作为总统的关键管理优先事项并制定业绩指标。

(4) 在国家安全委员会的网络安全指挥部指定一名负责隐私和公民自由的官员。

(5) 召集政府相关机构，就在制定政策过程中遇到的网络安全相关事宜进行清除跨越部门界限的法律分析研究，并制定统一的政策指导，以明确政府各部门网络安全工作的任务、职责和权限。

(6) 发起一场促进网络安全公众意识的全国性教育运动。

(7) 制定美国政府对国际网络安全政策框架的立场，加强我们的国际伙伴关系。针对网络安全有关的各类活动、政策制定和机会，主动作为。

(8) 制定网络安全事件响应计划；展开对话，以加强公共-私营合作关系，着眼于理顺关系，并提供资源，便于其贡献和参与。

(9) 与其他总统行政办公室（EOP）实体合作，制定研发战略框架，侧重于以改变游戏规则的技术，以提高数字基础设施的安全性、可靠性、韧性和可信；为研究界提供获得事件数据的途径，便于其开发工具、测试理论，并找出可行的解决方案。

(10) 建立一个网络安全的身份管理的愿景和战略，以解决隐私和公民自由的关切，利用隐私增强技术保卫国家。

### 中期行动建议

(1) 针对各机构间对有关网络运行的法律解释和适用政策的不同意见，改进分歧解决程序。

(2) 使用管理和预算办公室（OMB）的项目评估框架，以确保各部门在实现网络安全目标时使用了基于绩效的预算编制。

(3) 增大对关键的教育项目和研发活动的支持，以确保国家在信息时代经济中的持续竞争能力。

(4) 制定一项扩大和培训人才队伍的战略，包括吸引和留住联邦政府中的网络安全专业人才。

(5) 确定最高效和最有效的机制，以实现战略预警，维持态势感知，以及向事件响应能力提供信息支持。

(6) 制定一套威胁场景和指标，用于风险管理决策、恢复计划和确定研发重点。

(7) 制定一个政府和私营部门之间预防、发现和响应网络事件的协作流程。

(8) 建立与网络安全相关的信息共享机制，并解决对隐私和专属信息关注，使参与信息共享的各方都能受益。

(9) 制定在自然灾害、危机或冲突情况下用于应急通信能力的解决方案，同时确保网络的中立性。

(10) 扩大与主要盟国之间的网络事件和脆弱性信息的共享，寻求能够改善经济和安全利益且同时保护公民自由和隐私权的双边和多边协定。

(11) 鼓励学术研究和工业实验室合作，建立成果转移路径和激励机制，促进研究和技术开发创新成果的应用。

(12) 从基础设施的目标和研发框架出发，确定国家标准化工作及参与国际标准化组织有关工作的目标。

(13) 实施互操作的身份管理系统，以建立对网上交易的信心，并增强隐私保护。

(14) 完善政府采购战略，改善市场激励措施，鼓励采用安全与强健的硬件及软件产品、新的安全创新成果以及安全管理服务。

---

## 二十二、网络空间国际战略

——维护网络世界的繁荣、安全与开放

美国白宫

2011 年 5 月

---

## 序

网络空间及其相关技术使得来自不同国家、种族以及持有不同信仰以及观点的人们能够相互沟通、交流、合作。当前，网络空间处于前所未有的繁荣发展阶段。美国公司可以通过互联网连接在世界任何地方发展业务，为美国人民提供无数的就业机会。非洲的农村妇女能够将自己的工艺品出售给拉丁美洲的家庭，从而推动更广泛的经济的发展。欧洲的实验室可以通过亚洲生产的硬件、北美洲编写的软件进行实验研究，而来自澳大利亚和中东的学生可以通过视频会议一起学习。通过信息技术，全球的公民都有能力使他们的政府更加开放，更能体察民情。

今天，随着越来越多的国家和人民开始使用网络，我们面临一个选择：是共同努力挖掘实现更大繁荣和安全的潜力，还是为了狭隘的利益过分担心，从而限制其发展。网络安全不是我们的最终目的，使网络为创新发展、市场繁荣和生活改善做出贡献才是我们的政府和社会的义务。如今，犯罪行为已经向数字世界转移，我们将共同面对并坚持以下原则：严厉打击网络犯罪，同时确保言论和集会自由、公民隐私以及信息的自由流动。

数字世界不再是一个没有法律监管的区域，也不是一个微小的特殊区域。它是各国间责任、公正以及和平逐步规范，并开始由人民所掌控的地方。社区组织就是一个很好的例子，由民间社会、学术界、私营部门以及政府部门共同、民主实施有效管理。最重要的是，网络空间自产生以来，一直在成长、发展，促进了社会的繁荣、安全和开放，这也是我们为什么在国际环境中重点去保护它的根本原因。

正是本着这一精神，我提出美国的“网络空间国际战略”（以下简称“战略”）。这不是本届政府第一次围绕这些技术提出相关政策挑战的解决方法，但这是第一次提出美国将与国际伙伴一起围绕网络上的各种问题制定一系列统一的战略方针。因此，“战略”纲要不仅是对未来网络空间的展望，也是其实现议程。“战略”为我国国内外的合作伙伴理解优先事项、认识网络空间的属性从而减少面临威胁提供了重要参考。

互联网自身并不会创造一个国际合作的新时代。但是，作为这项工作的受益者，我们可以共同努力去建设一个开放的、互操作性强的、安全可靠的未来网络空间。这就是我们所追求的，同时诚邀所有的国家和人民加入我们，投身于这项工作之中。

——奥巴马

## 1. 制定网络空间政策

“网络空间，这是一个我们每天都依赖的世界……它使得我们之间比人类历史上任何时期都存在更多的互联互通。”

——总统奥巴马，2009年5月29日

数字基础设施已经逐渐成为经济繁荣、研究活跃、军事能力强大、政府透明以及社会自由的脊梁。信息技术正前所未有地成为增进跨国对话交流和促进全球货物服务流通的有效手段。这些社会和贸易的关联已经成为我们日常生活不可或缺的一部分。一些赖以生存的关键基础设施，如电力和水资源供应、空中交通控制以及金融系统都完全依赖于网络信息系统；当前政府

能够通过电子政务提供合理的基本服务。社会和政治运动通过互联网能够提供新的更多样的组织和行动的方式。网络技术的应用呈现普遍性和全球性的趋势。对所有国家而言，基本的数字化基础设施正在成为或将要成为国有资产。

要充分实现网络技术给世界带来的好处，这些系统必须是安全可靠的。人们必须对数据能安全地传送到目的地充满信心。确保信息的自由流通、数据安全和隐私以及互联网络本身的完整性是美国和全球经济繁荣、安全和尊重人权的基本要素。

世界上几乎三分之一的人口在使用互联网，更多的人在日常生活中接触互联网。今天世界上有超过 40 亿个无线数字设备，在半个世纪前这个数字几乎为零。我们生活在一个难得的历史时刻，有机会去成功地构建网络空间，并保护美国公民和国际社会的安全。

这些技术将继续增强个人能力、促进社会发展，并为构建现代经济提供研究、发展和创新的基本要素，在其爆发性增长和发展的过程中必须保持开放性和互操作性的特征。这些都是需要支持的技术发展和建立有效的管理体系。与此同时，我们的网络必须是安全可靠的，它们必须依赖于可信任的个人、企业和政府，能够有效地抵御任意或恶意的破坏。

全世界必须共同认识到恶意行为者进入网络空间带来的严峻挑战，并相应地更新和增强我们的国家和国际战略。在网络空间进行的活动会对我们的现实世界产生相应的影响，我们必须建立相关的法律去抵御风险。一个开放的、可互操作的、安全可靠的网络空间的未来取决于国家对于那些意图动摇和破坏网络世界的人的认知和所采取的防范措施。

### 战略方针

美国网络空间国际战略的基础是相信网络技术对我们国家乃至世界有着巨大的发展潜力。在过去 30 年间，美国看到了这些技术给我们的经济和日常生活带来的革新和转变，也见证了网络空间中带来的剥削和侵略的挑战。为了去应对这些挑战，我们将发挥表率作用。美国将追求能够创新经济发展和改善生活水平的网络空间国际政策。在这项工作中，我们立足的基本原则不仅基于美国的外交政策，而且也从互联网未来的发展前景考虑。

### 立足机遇

美国致力于维护和增强数字网络为我们的社会 and 经济发展所带来的益处。

这些益处是具有多元化和影响深远的。对个人而言，计算机网络提高了生产力和社会的繁荣，帮助人们克服了一些缺点和不利因素，使得原本因为语言不同和身患罕见疾病的人能够集中，也使得相隔很远的家庭和朋友能够联系在一起；对团体而言，它们提高了对突发事件的反应能力，在帮助解决犯罪、揭露腐败、促进政治运动以及聚焦原本被忽视的问题等方面扩大了信息交流共享；对企业而言，开辟了新的市场，催生了数十亿美元的产业；对政府而言，能够提高透明度、效率以及便利性，有利于政府与人民保持密切联系；对国际社会而言，能够为新的全球市场空间提供基础，同时帮助共同面对灾难。信息流通越自由，我们的社会就会变得越强大。合理利用这些技术能够提升我们的能力，我们将努力扩大其覆盖面，改善和提高这些技术在国内外的相关应用。

### 认清挑战

美国认识到，网络的发展给我们的国家安全和经济安全以及国际社会的安全都带来了新的挑战。

这些挑战有多种不同的形式。自然灾害和事故能够破坏美国的电缆、服务器以及无线网络，技术挑战也具有同样的破坏性，一个国家屏蔽网站的方法可能引发更大的国际网络破坏。勒索、欺诈和剥削儿童会打击用户在在线商务和社交网络，甚至是人身安全方面的信心。对知识产权的窃取也威胁到了国家的竞争力和创新能力。这些挑战已经超越了国界，进入网络空间的低成本以及建立匿名的虚拟身份也为罪犯提供了“安全的避难所”。随着传统的冲突形势延伸进网络空间，更广泛地来看，网络安全威胁甚至危及到了国际和平与安全。

### 遵循原则

美国将遵循我们的核心原则去面对这些挑战。

我们的政策是承诺保持最好的网络空间环境和维护自身的原则。我们的网络空间国际战略反映了我们的核心原则：保护基本自由、隐私和信息流动自由。

(1) 基本自由。我们承诺的言论和集会自由，不是以牺牲公共安全和公民的保护为代价的。在这些公民自由中，国际公认的“基本自由”，指通过任何媒介和不论国界去搜索、接受以及传递信息和思想的能力，从未像现在这样重要。作为一个国家，我们不能无视那些有邪恶意图的互联网用户，必须要意识到网络空间的自由言论也必须适当地调整。例如，儿童色情、煽动暴力或者组织恐怖活动在现实中是明确禁止的；同样，这些行为在互联网也没有存在的空间。美国将从自身的核心价值观出发继续去和这些行为作斗争——具体地去解决这些问题，而不是关于互联网的价值面向社会进行全民投票。

(2) 隐私。我们的策略是和保护公民的利益和隐私是相匹配的。随着公民在公共和私人生活中越来越多地使用互联网，他们对自身的隐私也寄予期望——希望理解他们的数据如何被使用以及如何确保数据能够被公正地处理。同样，他们期望去保护自己远离诈骗、盗窃以及网上潜在的安全威胁，希望利用法律手段去处置、追踪和起诉意图使用网络去损害他人利益的人。美国主要通过相应的调查机构进行执法，致力于确保双方的平衡，同时通过相应的司法审查和监督来保护个人权利，确保法律法规的一致性。

(3) 信息流动自由。国家并不需要在信息流动自由和网络安全之间做出选择。网络安全最好的解决方法是动态地、适应性强地对网络性能产生最小影响。这些安全工具系统没有削弱创新，也没有限制言论或者集会的自由，更没有阻碍全球的互操作性。相反，我们看到其他方法，如国家级过滤器和防火墙只是提供了安全的假象，阻碍了互联网作为具有开放性、互操作性、安全可靠性的交流媒介的有效成长与发展。商业上也是如此，网络空间必须保持一个鼓励创新、创业和勤奋的公平的竞争环境，而不是去任意破坏信息自由流动从而产生不公平的情况。美国致力于制定国际倡议和标准，加强网络安全并同时维护自由贸易和信息自由流动，这些是我们的全球责任，同时也是我们国家所需要做的。

很多时候，一些原则的特性与有效执法、网络的匿名性、儿童的保护以及基础设施的安全性是不相容的。事实上，良好的网络安全可以增强隐私性，针对广泛认可的非法行为的有效执法能够保护基本自由。民事裁定要忠于保障人民权益、稳定全球市场、控制恶意行为者产生国际影响，法律法规既维护了我们国家的安全，也推进了共同的价值观。

## 2. 网络空间的未来

设想一下，未来我们可以从地球上任何一个角落、以每个公司和家庭都能承受的价格安全可靠地访问互联网。通过全球可信无缝网络，我们可以随时随地与世界各地的朋友、同事进行即时通信。大量的知识、新的观点和丰富多彩的辩论等这些用自己的语言表述的内容，通过开放的数字翻译可以跨越国界自由传输。促进农业发展的新技术和促进公众健康的信息，可以在最需要的人群中共享，这一切都得益于全球专家和研发人员的协作。这是美国憧憬的网络空间的未来，我们将努力实现。

在未来的网络空间里，个人和企业可以快速方便地获取必要的工具来建立视频会议，域名和地址都是可用的、安全的、好管理的、不存在烦琐的许可和令人担心的个人信息泄露问题。国际上最好的工程师一起工作，开发新标准和信息系统，使网络更快、更可靠，更具创新性和无缝性。高新技术企业与他们的客户一起工作，可以提供更安全、更可靠、更符合客户需求的软件、硬件和服务。

在未来的网络空间里，大学和企业可以自由地研发新概念和新产品，因为它们知道即使是在共享网络中，它们的知识产权和有价值的数据也是绝对安全的。每个人都清楚地知道他们的计算机存在的威胁，并且可以使用易于操作的方法保护系统。私营公司认识到维护网络的安全和稳定也是在保护自己的投资。当网络安全事件需要政府干预时，官员可以尽早地检测威胁，实时地共享数据，阻止恶意软件的传播，最大程度地降低破坏程度，同时也能维持信息不间断传输。当涉及国际犯罪调查时，执法机构能够进行跨国合作，维护和分享证据，并把罪犯绳之以法。

未来的网络空间不仅提供了更繁荣、更可靠的网络，而且增强了国际安全和持久的和平。在网络空间里，国家要负起责任，不遗余力防止他人破坏网络，还要消除犯罪分子的避风港。国家认识到必须保护网络基础设施不会受到干扰甚至破坏。通过双边、多边和国际合作，将世界上更多的国家带入信息时代，达成维护互联网及其核心属性的共识。

美国已经和越来越多的合作伙伴为网络空间的未来奠定了基础。但仅靠美国自己不能完成这个目标。尽管这可能是一个动态的、漫长的且需要消耗大量资源的过程，国际社会必须携手合作支持这项长期的投资。我们之所以要这样做，是因为我们清楚地认识到未来的网络空间不仅代表国家的利益，也是国际社会的共同目标。我们看到了全球网络互联的最大利益和最小风险，我们的成功将开启信息技术新的纪元。

### 探索未来

我们期待的未来网络空间应该具有激励创新、增强个人权益的作用；它是连接个人与社会的纽带；它促进政府变得更好，并扩大问责制；它保障基本自由和个人隐私；它建立互信，明确行为准则，并增强国家和国际间的安全性。为维护这种网络空间的环境，国际合作不仅是最佳实践，更是首要原则。

### 我们的目标

美国将与国际社会一道努力促进建立**开放、互操作、安全、可靠**的信息和通信基础设施，以此来支持国际贸易、加强国际安全，并促进言论自由和创新。为了实现这一目标，我们将建立和维护一种网络空间环境，通过**负责任的行为规范**来指导各个国家的行为，维持伙伴关系，支持网络空间的法律法规。

#### (1) 开放和互操作性使网络空间更为强大

数字创新的核心是给网络设备增加新功能的能力。数字系统的开放性决定了它的爆炸式增长、迅猛的发展和久经考验的重要性。计算机和互联网接入已经遍及每个国家，互联网基础设施的可用性正在稳步提高，价格却持续走低。为继续满足不断增长的网络用户的需求，硬件和操作系统制造商必须继续把全球各地尽可能多的开发人员都动员起来。企业在推进私有软件不断取得创新的同时，我们同样也赞赏开源软件运动的活力。开源软件给开发者和消费者提供了以社区为导向的解决方案，从而满足他们的需要。

美国支持互联网端到端的互操作性，从而使全世界人民可以通过技术手段交流知识、思想并相知相识。信息的自由流动取决于互操作性，这是在突尼斯信息社会世界首脑峰会上 174 个国家所达成的共识。与全球开放性和互操作性相反的是那种互相隔离的网络。由于少数国家的政治利益驱动，使得世界上大量的人口无法使用高端的应用程序及获取丰富的内容。达成信息和通信技术国际标准的共识，是保持开放性和互操作性、发展数字经济并推动我们社会前进的重要一步。

#### (2) 安全可靠保障网络空间持久发展

互联网系统必须得到我们的信任才能使网络空间具有持久性。用户需要有足够的信心去相信他们的数据被安全地转换和储存，以及可靠地传输。一个有效的政策往往需要从各个方面采取行动，由社会各阶层共担责任，并通过各个国家的终端用户共同合作。

降低网络的脆弱性需要强有力的技术标准和解决方案、有效的事故管理、可信的硬件和软件以及安全相关的供应链。全球范围内降低这种脆弱性风险需要有效的执法、国际公认的国家行为准则、建立信任和提高透明度、积极主动的外交和相应的威慑力。最后，事故响应需要加强私营机构和国际社会双方的合作和技术信息的共享。这项工作不可能由某个国家和部门单独解决，它需要所有国家及其人民一起承担这份责任与义务。

网络的稳定性是全世界繁荣昌盛的基石，确保网络的稳定不仅是一个技术性问题。在经济方面，当我们鼓励国家和企业维护网络稳定、并明确义务的同时，我们必须促进经济的可持续增长，并加大在国内和国外的基础设施投资。在政治方面，我们必须加强对网络基础设施的尊重，使得国家之间的争端不会成为干扰甚至破坏网络的借口。在社会方面，我们必须让最终用户意识到，采用一种安全可靠的方式维护和操作他们的设备是自己的责任。

#### (3) 通过国际行为准则保持稳定性

美国将与志同道合的国家建立一个大家期待的网络空间环境，准确说是一项行为准则，即制定外交和国防政策并引导国际合作。在过去的 20 年里，互联网作为一种社会媒介以前所未有的速度快速增长。我们的社会越来越依赖网络信息系统去控制重要基础设施，也越来越依赖现代生活必不可少的通信系统。越来越多的证据表明，政府正在寻求一种通过网络空间行使传统国家权力的途径。在网络空间中，对于什么样的国家行为是可以接受的，目前还没有相应的准则。为了弥补这个不足，我们将努力在什么行为是可接受的问题上达成共识，并与那些认为



这种共识对其国家和集体利益至关重要的国家建立伙伴关系。

(1) 准则的角色。从国际关系的角度看，在什么样的行为是可接受的问题上实现互信与谅解有利于促进国际稳定。当国际社会需要采取必要措施时，它可以作为国际行动的基础。遵守这些准则，使得国家行为具有可预测性，也有助于避免因误解而可能导致的冲突。

在网络空间制定国家行为准则并不意味着要重新制定现有的国际法规，更不会使现有的国际准则过时。无论是和平时期的还是战争年代，那些早已存在的约束国家行为的国际准则同样也适用于网络空间。尽管如此，网络技术的独特属性使得我们需要进一步说明这些准则如何应用，以及哪些准则需要更多的互信与谅解。我们将继续与国际社会一起努力，凝聚共识，明确如何将行为准则应用于网络空间。我们认为这种努力中重要的一步是给予网络空间广泛的期望，期待国际行为的和平与公正。

(2) 准则的基础。准则有利于促进有序与和平，提高人类的基本尊严，促进经济自由竞争。这样的准则是任何国际环境所必需的。这些准则为各国决定如何履行他们在网络空间中传统的国际义务奠定了基础。在许多情况下，这些准则也反映了无论什么环境下国家都应履行的职责。现有的支持网络空间的准则包括以下几项。

- 维护基本自由：各国必须尊重言论和结社基本自由，无论是网上还是网下。
- 尊重知识产权：各国应承诺并通过国内法律以尊重和保护知识产权，包括专利、商业秘密、商标和版权。
- 重视隐私：当个人使用互联网时，其隐私应受到保护，不受到任意或非法的干涉。
- 打击犯罪：各国必须识别并起诉犯罪分子，维护法律和风俗习惯，剥夺犯罪分子的避风港，并及时配合国际刑事调查。
- 自卫权利：与联合国宪章一致，各国在网络空间遭遇到一定的侵略行为时，拥有固有的自卫权利。

源自传统的国家行为准则，具体到网络空间时更多的是责任，特别是侧重于维护全球网络功能和提高网络安全的责任。这些责任很多是基于互联网技术。由于互联网的核心功能依赖于可信任的系统（如边界网关协议），各国必须承认其技术层面的决策会造成国际影响，并尊重彼此的网络和国际互联网。同样地，在设计下一代网络系统时，我们必须依靠健全的技术标准和管理结构去实现共同利益，而不是依靠那种提高国家威望的强权政治方式。一些新兴的准则对网络空间也至关重要，包括以下几项。

- 全球互操作性：各国应在其管辖权内采取行动，确保互联网端到端访问的互操作性。
- 网络稳定性：各国在配置该国网络时应尊重信息的自由流动，确保不随意干涉国际互联网络的基础设施。
- 可靠地访问：各国不任意剥夺或干涉个人接入互联网或使用其他网络技术的权力。
- 多利益相关方治理：互联网治理活动绝不能仅限于政府，而应包括所有的利益相关者。
- 网络安全尽职调查：各国采取负责任的行动来保护信息基础设施，并保障国家系统的安全不受损害或滥用。

网络空间是一个动态环境，国际行为必须立足于负责任的国内治理、和平的国家间行为和可靠的网络管理。随着这些观念的发展，美国将促进并充分参与磋商，推进互联网政策的制定，增强在国际对话中各个议题的共识。

(4) 我们在未来网络空间的角色

为了实现这个未来网络空间，并积极推进规范和准则，美国将综合外交、国防和发展三方

面来提高网络的繁荣性、安全性和开放性，这三个方面是我们重点努力的方向。在 20 世纪后半期，美国致力于建立一个新的战后国际经济和安全合作体制。在 21 世纪，我们将努力实现在这种合作精神和集体责任下的和平可靠的未来网络空间。

### 外交：加强伙伴关系

在保持网络空间自身的优势和特点的同时，要扩大和平与安全原则，这就需要加强伙伴关系和增加主动性。我们将以坦诚和迫切对话的方式参与国际社会的活动，围绕负责任的行为准则在网络空间和国际行为上达成共识，在国内和国际社会建立一个网络空间稳定体系。

#### 外交目标

美国将努力为这样的一个国际环境创造激励机制，在这个环境里，对开放、兼容、安全、可靠的网络空间的内在价值达成共识，利益相关者应一起工作。

通过我们的国际关系和从属关系，我们将努力确保尽可能多的利益相关者融入到未来网络空间中，因为网络空间将使经济、社会、政治和安全等方面受益。我们通过与国内外私营企业的有意义合作来支持这项工作。

分布式系统需要分布式的行动，并且没有单独的机构、文档、安排或者工具能够解决世界网络化的需要。无论对于终端用户、私营的硬件和软件提供商、互联网服务提供商还是区域、多边、多利益相关者，在帮助网络空间满足全部潜力的方面都是很重要的。

特别是在国际舞台上，各国在维护和平与稳定、赋予创新、维护经济和国家安全利益、保护和促进公民个人权利等方面应该发挥持久的作用。在我们的国际事务中，美国将致力于建立一个国际期望的环境，该环境定位于外交和国防政策，并用来加强我们的国际关系。

(1) 双边和多边的伙伴关系。我们将在与各国双边基础上，对我们政府和人民有重要性的网络空间问题开展合作。关于建立网络空间行为准则，必须以与志同道合的国家建立清晰的准则为开端。我们将努力寻求广泛的合作伙伴，在广泛的双边对话范围内包含网络空间的议题，该对话跨越各级政府和大范围的活动。在网络空间出现的挑战方面，我们将推进共同行动。此外，我们将积极参与发展中国家的对话，确保在这些问题上发声并被各国听到。

(2) 国际组织和多利益相关方组织。区域组织对其成员在解决网络安全问题上是非常有效的，他们将在制定和推广行为规范方面扮演越来越重要的角色。我们将继续利用我们在这些组织中的成员以及更加广泛的国际组织，来发展适合每个组织的专业知识，为会员实现实实在在的利益。美国赞扬这些努力，并承认这些组织的独特贡献，这些组织包括私营企业、民间社会、学术界以及多利益相关的政府，代表了整个互联网社区。

(3) 私营部门的协作。私营部门已经发挥了在国际和多利益相关者组织中的重要作用，我们将继续利用现有的合作机制，吸收行业合作伙伴。特别是，我们将促进基础设施所有者和经营者紧密合作，保护网络空间的优势和特点，避免不必要的障碍，并确保网络空间的和平与安全。我们还请私营企业作为必不可少的多利益相关者参与互联网的治理，并会继续在相关论坛上倡导互联网的包容性。

### 国防：劝阻和威慑

美国将捍卫自己的网络，面对无论是来自恐怖分子、网络罪犯，还是来自其他国家及其代理人的威胁。同样重要的是，我们将设法鼓励良好行为并劝阻和制止那些在网络上威胁和平与

稳定的行为。我们将根据国家和国际网络警惕应对方案的重叠政策去实施。我们将尽力利用我们的法律和原则去保护公民的自由和隐私。

### 国防目标

美国将同其他国家一道鼓励负责任的网络行为，反对破坏网络和系统的行为，劝阻和制止恶意行为，并保留采取必要和适当措施的权利来保护这些重要国家资产。

#### (1) 劝阻

保护如此之高价值的网络需要很强的防御能力。美国将继续增强我们的网络防御、承受和从其他攻击中恢复的能力。对于那些造成严重损害的攻击，我们将采取行动来隔离和减少对设备的干扰，降低对网络以及潜在的级联式的影响。

(1) 国内实力。确保我们的网络和信息采取一致的国家行动，该行动跨越了整个政府与私营企业和公民个人的合作。10年来，美国已经形成了一种网络安全文化，研制了对风险事件有效缓解的设备，我们继续强调，无论是对公共部门还是私营部门，采用良好信息技术的系统将减少我们国家的脆弱性并增强网络和系统。我们已经建立了安全事件响应小组，在政府、重点行业、关键基础设施部门和其他利益相关者之间共享信息。此外，我们不断寻求新方式来加强与私营企业的伙伴关系，以加强安全性。

(2) 国外实力。这种防御模式在国际上通过教育、培训和持续业务和政策关系已成功地被分享了。今天，通过和发展中国家在技术和军事防御领域的合作，各国共享前所未有的对事件的认识和响应能力，拒绝攻击者对我们的国家和国际网络造成持久的损害。然而，全球分布式网络需要全球分布式预警能力。我们必须继续在全球范围形成新的计算机安全事件响应能力，并帮助它们加强计算机网络互联和防御能力。美国一直在帮助不发达的国家建立防御能力，并成为我们的伙伴合作，我们将重点加强这方面的建设，与朋友和盟国建立关系，提高整个国际社会的集体安全性。

#### (2) 威慑

美国将确保，攻击或利用我们的网络所带来的风险将远远超过潜在收益。我们充分认识到，网络空间的行为的影响可能超出网络的范围，这类事件需要采取自我防卫响应。同样，各国的网络连接更加紧密，对一个国家的网络攻击可能会远远超出其国界。

当罪犯和其他非国家行为者威胁我们的国家和经济安全时，国内威慑要求所有国家都有相关程序能够对那些在国内或国外的侵犯或破坏网络的人进行调查、逮捕和起诉。在国际上，执法组织必须彼此呼应，尽可能保存对调查至关重要的数据，与立法机构和司法部一起合作，并促进遵循正当程序和法律规定，即关于网络犯罪的布达佩斯公约中的所有关键条款。

当确认网络空间中敌对行为后，美国将做出回应，就像我们回应对我们的国家其他威胁一样。所有的州都拥有自卫权利。为了保卫我们的国家、我们的盟友、我们的合作伙伴和我们的利益，我们保留使用一切必要手段——外交、信息、军事、经济以及适当和适用的国际法律的权利。在这样做时，我们将尽量不使用武力，我们将采取一种反映我们价值观和增强我们合法性的行为方式，寻求尽可能广泛的国际支持。

### 发展：建立繁荣与安全的网络空间

美国将继续证明“互联的世界是有益的”这一信念是普遍的。一个具有开放、兼容、安全、

可靠等优点的网络空间应比现在的网络空间更具可用性。作为世界首位的信息经济体，美国致力于确保技术资源或专利知识所有者的权益。

我们国家能且将要在为建立、保护新的和现有的数字系统而提供知识和能力中将扮演重要角色，且目前正在这样做，作为一名负责的利益相关者努力在各个国家之间建立共识。实现能力建设，这个目标不是一个短期的开支，而是一个长期的、明智的投资和承诺，我国政府将持续参与。

#### 发展目标

美国将推动网络空间安全能力在国外的建设，通过双边和多边会议，让每个国家都有能力保护自己的网络基础设施，加强全球网络工程，并在建设更为开放、兼容、安全、可靠的网络方面建立密切的合作伙伴关系。

##### (1) 建立技术能力

网络接入技术日益成为发展的基本需求。政府和工业界提出了很多有意义的方法，以加强与未开通服务且人口稠密地区的终端用户的连接。国际信息基础设施的不断成熟和扩大，为更多国家进入全球信息流提供了机会。全球范围内网络的不断增长，接入的用户不断增多，丰富了国际社会交流，然而在传统及网络空间安全等问题上的合作也提出了新的挑战与机遇。这些能力很大程度上将来自于私人部门的投资，美国将与各国政府及业界进行合作，营造友好的气氛，并可以一起解决国家发展的核心需求。

政府是重要的因素，决定着这些新的互联网产品发挥积极的作用还是其潜能被浪费掉。我们在互联网建设方面的努力使很多国家受益，这些国家的愿望是通过技术使国家建设的更加繁荣，并进一步加强社会的凝聚力，而不是通过限制访问来达到政治上的控制意图。出于这个原因，美国将通过支持技术项目加强安全和商业贸易，保障信息流动的自由，促进网络全球互用。

##### (2) 建立网络安全能力

繁荣不能建立在担心和不可靠的基础上，美国致力于帮助各国一道提高自己的网络空间安全技术开发能力。加强国家级网络空间的安全是发展中国家当前及长远的利益，随着更多国家都有能力对付来自国内外的威胁，我们应建立信心，携手合作打击跨境非法滥用信息技术犯罪。此外，还必须培养有能力的国际研究人员能够承担下一代网络空间安全的挑战。

认识到网络安全是一个全球性的问题，必须与一些国家一起努力解决，我们将扩大和规范网络空间安全的能力建设，更加注重提高认识、法律和技术培训，提供政策支持。这些方案的解决不是纯粹的技术问题，我们将与各国一起努力认识到网络空间安全是个宽泛、更严重的挑战，协助它们发展自己的国家战略，并建立涵盖整个行业范围的网络安全保障能力，建立计算机应急响应小组，实施国际执法和防务合作，促进国内、国际私营企业和民间社会及团体的关系。

##### (3) 建立政策关系

美国网络空间安全能力建设援助是一种投资、一个承诺，并作为对话或合作的重要契机。随着国家一同深入地处理网络空间问题，我们希望对话能从建立网络空间安全能力，进一步向经济、技术、执法、国防以及共同关心的外交问题方面发展。我们也将促进发展中国家在网络空间安全方面的合作关系，同时使用区域论坛和拥有专业知识的技术机构继续共享最佳实践的方法、经验教训以及国际技术交流。

### 3. 政策优先

美国将继续采取行动，为我们的公民以及全世界人民在国内外建立和维持开放、互操作、安全、可靠的网络环境。我们采取的方法遵循基本原则，以总体目标为导向，由本文概述的政策所支撑，它们共同形成了美国网络空间国际战略的基础。

为了充分发挥未来网络空间的潜力，美国政府在 7 个相互依存的领域组织计划了系列行动，每个行动都要求我国政府与国际伙伴、私营部门相互合作。整体而言，这些行动构成了我们战略框架内的行动线。

美国政府的许多部门和机构已经开始参与行动了，正在为这项重要工作添砖加瓦。这些正在实施的未完成的计划体现了在网络空间中的政府部门和机构的具体责任，并且它们上下一致努力完成计划。这里提到的政策优先是这些具体计划的指导意见，是过去、现在和今后的重点领域，需要全国高度关注和资源配置。

#### 经济：推动建立国际标准、创新和开放市场

为了确保网络空间继续服务于我们的经济和创新，我们将：

(1) 维持基于全球互联网络的自由贸易环境，鼓励技术创新。正如信息的自由流动对我们网络运行的重要性，在信息时代，自由贸易促进了技术创新和市场的发展。全球互联网的特征，可以大致归结为较低的成本和全球可用计算机及网络技术。在这些市场中的竞争推动了技术创新，尽管自由贸易环境使制造商保持价格和标准竞争优势。重视技术开发的国际标准和贸易是维持开放市场必要环节，这样可以促使领先的技术公司快速从他们创新产品和服务中获益。未来几十年中，制造业技术将不断全球化，而且会从我们的网络和消费者中获益。美国将努力维持自由贸易的环境，特别是在高科技领域，以确保未来的创新。

(2) 保护知识产权防止窃密，包括商业贸易秘密。网络全球化促进了创新，同时为工业间谍活动以及窃取知识产权和商业信息开辟新的途径。通过网络空间可以从企业、大学和政府中盗窃大量的信息，这些被窃取的信息和技术等同于数十亿美元的损失。个人事件往往被隐瞒或未被发现。不公平的竞争导致整个公司的破产，而对国家的影响可能会更厉害。持续的知识产权盗窃，无论是由罪犯导致的，还是外国公司或国家行为，都可以削弱其在全球经济中的竞争力和商业创新的机会，美国将采取措施，发现并应对此类行为，以帮助建立一个国际环境，确认这种行为是非法的、被禁止的而且要参与者承担相应的责任。

(3) 确保由技术专家决定的互操作和安全技术标准的首要性。建立国际化的、自愿的、达成共识的网络安全标准，部署基于以上标准的产品、程序、服务，是构建互操作的、安全和韧性的全球基础设施的基础。公共-私营部门必须共同努力开发、维护和执行这些标准，支持国际标准和合格评定制度的建立，为国际贸易和电子商务清除障碍。国际网络空间标准是以自愿和协商一致为基础，服务集体利益，鼓励创新，促进互用性、安全性和韧性，提高网上交易的信任和刺激全球市场的竞争。美国将加强公共-私营部门之间的合作，以确保产品和服务的国际标准的规定颁布。

#### 保护我们的网络：加强安全性、可靠性和韧性

开放的环境下，网络空间的安全性对国家和经济的安全是至关重要的，因此我们将：

(1) 促进双边和多边组织以及多国合作伙伴之间在网络空间开展合作，特别是关于国家行

为规范和网络安全合作。越来越多的国际组织采取网络安全和其他网络空间的措施，美国将继续推动这一重要工作，将建设网络空间纳入工作范围，以满足不同成员的需要。已经将网络空间议题列入有关工作议程上的包括以下国际组织：美洲国家组织（美洲组织，OAS）、东南亚国家联盟（东盟，ASEAN）区域论坛（ARF）、亚太经济合作组织（亚太经合组织，APEC）、欧洲安全与合作会议（欧安组织，OSCE）、非洲联盟（非盟，AU）、经济合作与发展组织（OECD）、八国集团（G-8）、欧洲联盟（欧盟，EU）、联合国（UN）以及欧洲委员会。为了确保有一个有效的工作体制结构，美国将继续和这些组织合作，巩固关键网络空间的活动的区域和国际共识，包括准则。我们会期待多利益相关方的合作和建立共识的论坛，以进一步推动互联网政策的制定。我们欢迎扩大这一项工作的区域范围，特别是非洲和中东地区，进一步推动全球范围的合作。

（2）对减少美国网络的入侵和破坏。未经授权的网络入侵威胁各经济体的完整性，危害国家安全。美国政府机构正在与私营部门合作，保护创新防止工业间谍活动，保护联邦、州和地方政府的网络，保护低级经营环境的军事行动，并确保关键基础设施的安全以防入侵和攻击。特别是在能源、运输或财务系统以及国防工业基地，美国将寻求广泛的国际共识，尊重财产，注重网络稳定的，支持我们自己和我们的合作伙伴共同捍卫我们的网络，防止恶意攻击。

（3）确保信息基础设施稳健的事件管理、韧性和恢复能力。在一个相互联系的全球环境中，一个国家不牢固的安全系统会给其他国家带来风险，没有任何国家可以全面了解全球网络，当事件可能威胁到我们所有人的时候，我们有责任分享自己网络见解和与他人合作。由于我们将继续建立和加强我们自己的反应能力，我们将与其他国家扩大国际网络范围以支持更多的对全球态势的认知和事件响应能力，包括政府和行业。通过与国际伙伴信任网络的信息交换，美国政府将积极观察、警告和及时反应。我们将通过国际合作扩大这些能力，以提高整体可靠性。美国也将努力参与网络安全的国际合作，以提升和加强与合作伙伴建立的工作程序。

（4）通过行业咨询，提高高技术供应链安全性。关键网络和信息基础设施的运营依赖值得信赖的硬件和软件的实用性。供应链中的漏洞可以影响网络的完整性、可用性和保密性和它们包含的数据。这些缺陷损害经济和国家安全。美国将与业界及国际伙伴合作，制定保护信息系统和关键基础设施完整性的最佳实践。这样，我们将大大提高自由和开放的贸易依赖的全球化的供应链的安全。

#### **执法：扩展合作和法律规则**

为加强网络空间的置信度和帮助在线系统的开发者，我们将开展以下活动：

（1）充分参与国际网络犯罪的政策制定工作。美国承诺通过成熟的专业知识和有效推进网络犯罪政策实施的经验，积极地参加讨论关于网络犯罪的国际规范和措施如何在双边和多边论坛上发展。这些对话会整合现有的工作，如扩大《布达佩斯公约》的适用范围。美国将努力在法律执行政策和有成效的政策对话中构建成功的伙伴关系。这是目前我们十分乐于参与的，同时各国也应积极培养责任意识并一起努力。

（2）扩大《布达佩斯公约》的范围，协调有关网络犯罪的国际法律。当侦查和起诉网络犯罪案件的时候，美国及其盟国通常需要依赖其他国家的帮助并一起合作。当每个国家都有共同的网络犯罪相关法律时，这种合作是最有效和有意义的，因为这样有利于证据共享、引渡以及其他类型的协调。《布达佩斯公约》在网络犯罪方面提供了一个起草和修订现有法律的模式，

而且它已被证明是在网络犯罪领域加强国际合作最有效的机制。美国将继续鼓励其他国家成为该公约的缔约国，将帮助目前非缔约国将这公约作为自己的法律基础，在短期内缓和双边合作，在长期内帮助它们成为《布达佩斯公约》的缔约国。

(3) 网络犯罪法律的重点在于打击非法活动，而不是限制互联网接入。网络空间的犯罪行为应通过有效的执法手段解决，而不是通过政策限制合法的访问或互联网上的内容。为了达到这个目的，美国政府在双边和多边的基础上确保各国能够认识到，在线犯罪可以通过阻止犯罪、抓获和惩罚犯罪者而解决，而不是扩大限制上网的范围，因为不断加大网络的限制将影响无辜的互联网用户。美国将和合作伙伴开展对话，并帮助世界各地建立各执法机构的能力。我们将整合这种方法，保护隐私、基本自由，合作创新，打击网络空间的犯罪分子。

(4) 阻止恐怖分子和其他犯罪分子，通过互联网实施行动计划、金融犯罪或攻击。在网络犯罪方面，美国具备多样化的国际能力建设和培训计划，以帮助执法和立法机构建立有效的法律框架和专业知识，来调查和起诉互联网上的恐怖分子和其他犯罪。防止恐怖分子通过“雇佣黑客”以及使用有组织的犯罪工具而增强自身能力，对国际社会而言具有很重要的优先事项，需要有效的网络犯罪相关法律。美国将致力于通过技术手段和国际合作，如金融行动特别工作组，来追踪和挫败恐怖分子和网络犯罪的金融网络。

### **军事：准备应对 21 世纪安全挑战**

我们决心在可能受到威胁的地方捍卫我们的公民、盟友和利益，为此我们将开展以下活动：

(1) 认识并满足军队对于可靠、安全的网络日益增长的需求。我们认识到，我们的军队越来越多地依赖于网络的支持，我们将会像保护其他重要的国防基础设施一样，在他人试图破坏我们系统的环境下，努力确保我们军队系统装备完整地运作。同其他国家一样，美国像重视捍卫自身核心原则和价值观一样重视捍卫我们的重要国家资产，并且致力于打击那些试图阻碍我们这样做的人。

(2) 建立和加强现有军事同盟，应对网络空间的潜在威胁。单靠一个国家难以实现网络安全，需要深层次国际合作以应对那些设法破坏或利用网络的恶意角色。这种努力始于北约及其成员国等这些我们最为亲密的盟友对于承认网络化系统的互联特性的认识，并将创造新的机遇与风险。展望未来，美国将继续在军事和民间领域与我们的盟国和伙伴共同努力，拓展态势感知并共享预警系统，以提高我们在和平或危机时期携手合作的能力，以及发展在网络空间集体自卫防御的方法和手段。这种军事联盟和伙伴关系将加强我们的集体威慑能力，并加强美国对其他国家和非国家势力的防御能力。

(3) 与盟国和伙伴展开合作，提高网络空间的集体安全。网络空间的挑战也为盟友和军事伙伴开创了新的协作方式。通过针对标准操作规程的建立共识，我们的部队可以通过协调和更进一步的信息交互来增强安全性。这些约定将减少对军事活动的误解和潜在的局势升级情况；对话和最佳实践的交流有利于增强合作伙伴的能力，诸如数字取证、劳动力建设、网络普及和弹性测试将成为工作的方向。美国将与志同道合的国家密切合作，利用杠杆效应来减少集体风险，并促进多利益相关方的有关倡议，阻止网络空间的恶意活动。

### **互联网治理：推动建立有效和包容的架构**

为了促进互联网治理构架有效地满足所有互联网用户的需求，我们将开展以下活动：

(1) 鼓励互联网上的开放与创新。互联网高效的信息传播能力已经成为现代消费、商业、

政治、科学和教育活动的核心。全球各国政府都已经认识到了互联网带来的价值，然而其中许多地方对信息自由流动的任意限制，或用其来镇压异议或反对活动。就像各国给出的理由各式各样，这些限制的方法和执行手段差别很大，但我们不应为适应决策而重新设计互联网的管理或技术架构，这将违反基本自由，或者不必要地导致扼杀创新。有效的、具有包容性的互联网治理应当是可以保证，严重不符合网络管理国际规范的角色将通过技术或治理结构被排除在外。维护、增强和提升对开放、全球化的互联网接入是一项明确的政策优先事项。美国将继续通过与多利益相关方机构和组织、有关政府和非政府组织签订协议以推进上述目标的实现。

(2) 维护全球网络安全和稳定，包括域名解析系统（DNS）的安全稳定。鉴于互联网对于世界经济的重要性，网络及其相关基础设施以及域名解析系统（DNS）的稳定与安全显得至关重要。为了确保持续的稳定和安全，我们和全世界其他国家将继续认可此领域相关组织和技术专家等利益相关者对于互联网运行所做的贡献。美国认为这些有效的资源调动促进了互联网的成功，并将继续支持这些多方利益相关方的工作。

(3) 促进和增强多方利益相关者讨论互联网治理问题相关活动。互联网分散、合作以及分层的架构体现了社会和技术组织模式，以上每个特质都奠定了互联网为人们带来的益处。互联网驱动着自由的创新，促进着经济的发展。互联网驱动着言论和活动的自由，推动着政治社会的发展以及世界范围内的民主社会运作。美国坚定地坚持我们的信念，即当国际社会需要去会讨论一系列互联网治理问题的时候，必须在多方利益相关者之间进行对话；我们将继续支持互联网治理论坛这样成功的载体，因为它提供了非政府利益相关者与政府平等的讨论的场所，体现了互联网自身开放与容性的本质特征。

#### **国际发展：建立能力、安全和繁荣**

为了促进全球网络技术带来的益处，增强我们的共同网络的可靠性，并建立网络空间的利益相关者责任共同体，我们将开展以下活动：

(1) 为寻求建立技术及网络安全能力的国家提供必要的知识、培训及其他资源。在一个相互关联的世界，互联网带来的益处不应该受到国界的限制。十多年来，美国致力于弥合各国之间的差距，已经帮助其他国家获得资源及职业技能，以获得其在技术和网络安全能力上的核心能力。我们的目标是通过我们的经验给其他国际以借鉴，特别是将网络安全成为其国家技术发展的方向。由于需求的数量与差距巨大，我们的计划包括支持事件管理国家能力、建立公共或私有的伙伴关系、增强控制系统的安全性、起草有效的调查和起诉网络犯罪的法律、制定和实施提高网络安全意识以及建立网络安全的国家文化。我们的工作已经通过对外援助双边进行，如与美国电信培训机构提议的公共-私营创新合作。近些年来，我们已经使这项工作在美国国家组织（OAS）、亚太经合组织（APEC）以及联合国（UN）等多边组织中推进。美国将扩大这些合作，在关注关键需求支持国内私有部门投资，并在今后的工作中用建立新的合作。

(2) 不断发展并且定期共享国际网络安全的最佳实践。目前，各国已经不再需要专门通过尝试与纠错的模式发展网络安全。我们与其他几十个国家以及众多的多边组织制定和分享网络安全的最佳实践，以帮助我们做出明智的投资并制定有效的政策。美国将与产业界开展密切合作，建立伙伴关系，继续定义、发展和完善最佳实践和技术标准，并将在促进它们接受我们的认识方面积极拓展工作。我们将进一步促进科学和技术研究的合作，以增强网络安全相关工具和能力。

(3) 增强国家打击网络犯罪的能力，包括针对执法人员、法医专家、法学专家以及立法者



的培训。由于很多犯罪案例使用了计算机网络，相关证据和犯罪目标位于国外，在应对严重犯罪和国家安全方面，各国政府经常需要依赖彼此间的合作，以开展更为广泛地技术和调查援助。犯罪威胁可能来自任何与我们有网络连接的国家，合作调查时，很多国家在能力方面都需要大量协助。通过提供相关培训，我们将提升执法者的对于技术的理解能力，这种接触会有效地增加执法合作和相互援助。美国将继续通过在各地提供培训以实现我们的目标，并在非洲、亚太经合组织（APEC）、东盟（ASEAN）、八国集团（G-8）和美洲国家组织（OAS）中继续推进此方面工作。

（4）与各国政策制定者建立关联，增强技术能力建设，与专家及其在美国政府的对口部门提供定期和持续的联系。在过去的几年里，关注网络空间问题的决策者的增加为国际社会提供了一个新的对话渠道，开启了新的发展与安全措施，并加强了众多的双边关系。正如我们在发展中国家通过技术和网络安全能力建设进行的长期投资，美国将致力于就共同关心的问题的援助关系建立更密切的伙伴关系。我们已经在子午线会议等论坛中占据主导地位，以促进关键信息基础设施保护问题上的合作。美国欢迎更多的国家加入到对话中，因为它们将越来越多地在网络空间的未来投资，并将与我们的专家和决策者建立持久的关系。

#### **互联网自由：支持基本自由和隐私保护**

为了确保网络空间的基本自由和隐私保护，我们将开展以下活动：

（1）为民间社会行动者提供可靠、安全的言论和活动自由的平台。我们鼓励世界各地的人们使用数字媒体表达意见、分享信息、监督选举、揭露腐败、组织社会和政治运动，并谴责那些反对使用数字媒体技术、引起骚扰、不公平的逮捕、威胁或支撑暴力的人们。这种令人担心的文化不鼓励社会的其他人使用新技术报告、组织和交流想法。同样，我们应保护互联网服务提供商和其他通信供应商，它们担任了审查合法的言论的角色，常常成为中介赔偿责任法律制度的受害者。美国将不遗余力地倡导网络空间的言论活动的基本自由，将赋予民间社会行动者、人权倡导者以及数字媒体记者相关权利，鼓励各国政府解决网络空间的实际威胁，而不是让企业来负责限制任何不当的言论或信息自由流动。

（2）与民间团体和非政府组织开展合作，制定保障措施以保护互联网活动不受非法数字的入侵。促进民间团体和非政府组织的网络安全有助于确保数字时代言论和活动自由。对希望表达可能是不受欢迎的言论和意见的活动者、倡导者以及一线记者来说，网络安全显得尤为重要，他们的电子邮件账号、网站、移动电话和数据系统经常被破坏和入侵。美国将赋予他们保护自己的权利，以确保他们在 21 世纪新技术时代有能力行使自己的言论和活动自由的权利。

（3）鼓励保护有效的商业数据隐私的国际合作。保护个人隐私对确保经济社会对互联网的信任是十分必要的。美国有一个强大的实施隐私保护法的记录，以及鼓励多利益相关方政策的发展。我们正继续加强美国商业数据隐私结构，以适应网络技术迅速变化的步伐。我们认识到在商业环境中同时维持创新必要的灵活性，应用一般的隐私权原则是有很有效的。为了共同的目标和更进一步的合作，美国将致力于建设互相认可的法律以促进保护隐私和创新。

（4）确保互联网端到端的互操作性将对所有人开放。用户应该相信通过互联网传递的信息能在世界任何地方都能接收到。同样，在正常环境中，数据传递不在乎起始和目的地是否跨国界。只有确保信息在互联网传输的完整性，用户才能信任互联网，互联网才能一直作为不断创新的可靠的平台推动全球经济增长，并鼓励世界各地人与人之间的思想交流。美国将继续坚信互联网的全球性本质，坚持反对将互联网分裂为国家内部网，而剥夺个人从国外获取内容。

## 4. 展望未来

网络技术带来的益处不应仅被少数特权国家，或者这些国家内的少数特权阶层所享受。网络的连通性并不是其最终目的，必须建立网络空间，它开放创新、具备全球范围的互操作性、足够安全以赢得网民信任、足够稳定以支撑人们工作。

30 年前，几乎没有人可以理解互联网如何改变我们的工作和生活。在这么短的时间内，数百万人依靠互联网技术生存发展。超过 10 亿人通过互联网进行社交。这项技术推动社会向前发展，完成了前几代人无法想象的事情。为了我们自己，美国将继续激发全世界人们的创造力和想象力，我们无法知道下一个伟大的创新是什么，但是我们致力于创造这样一个蓬勃发展的世界。

本战略将为美国政府部门和机构更好地界定和协调在国际网络空间政策中所扮演的角色提供政策方针，更有利于未来工作的开展和规划的实施。本战略呼吁私营部门、民间社会以及最终用户通过合作、提高意识、行动来加强努力。最重要的是，邀请其他国家和人民加入我们来共同创造一个繁荣、安全、开放的网络世界。这些理念对于保护现有的网络空间、共同创造我们梦想的未来而言是至关重要的。

---

## 二十三、第 21 号总统政策令：关键基础设施安全和韧性

美国白宫  
2013 年 2 月

---

针对关键基础设施安全和韧性的总统令（PPD）开启了国家级团结一致的努力，以强化和维护安全、可靠且富有韧性的关键基础设施。

## 1. 介绍

国家关键基础设施为美国社会提供了基础性的服务。为了强化和维持安全、可靠和富有韧性的关键基础设施，包括资产、网络和系统，主动和协调一致的努力是必不可少的。这对公众信心以及国家安全、繁荣和幸福而言至关重要。

国家关键基础设施是多样且复杂的。它包括分布式的网络、不同的组织结构和运行模式（包括跨国所有权）、无论在物理还是网络空间都互依赖的功能与系统，涉及多级授权、职责和监管的治理结构。关键基础设施的所有者和运营者成为其运行及资产的主要风险管理者，并为这些资产制定有效的安全与韧性战略。

关键基础设施必须是安全的，必须能够承受所有的危险并能从中迅速恢复。为了实现这一目标，需要在国家战备系统中集成预防、保护、缓解、响应和恢复功能。

本令制定了关于关键基础设施安全和韧性的国家政策。这项工作是由联邦与州、地方、部落和领地（统称 SLTT）实体以及关键基础设施公共-私营所有者和运营者（后文简称为“关键基础设施所有者和运营者”）的共同责任。本令还优化和明晰了联邦政府中与关键基础设施相关的职能、角色和责任，增强了协调与合作。为了确保国家基本功能的连续性，联邦政府也有责任去保护其自己拥有的关键基础设施的安全和韧性，并组织有效的合作，为关键基础设施所有者和运营者已经开展的安全和韧性工作添砖加瓦。

## 2. 政策

这是美国加强其关键基础设施的安全和韧性、防范物理和网络威胁的政策。联邦政府应当与关键基础设施所有者和运营者以及 SLTT 实体协同合作，采取积极主动的措施来加强国家关键基础设施的安全和韧性，并考虑一切可能对国家安全、经济稳定、公共健康和安全的一个或多个方面造成不良影响的危险。与关键基础设施相关的这些工作应该努力去减少脆弱性，减轻后果的影响，识别并阻断威胁，以及加速响应和恢复工作。

联邦政府还应当与关键基础设施坐落在该国的国际合作伙伴协作，以加强美国国内外关键基础设施的安全与韧性。

美国应努力以综合、整体的方式来考虑关键基础设施的安全和韧性，以反映基础设施之间的互联性和互依赖性。本令还将能源和通信系统作为特别关键的系统，因为所有关键基础设施部门的运转都需要它们。

为加强关键基础设施安全和韧性，联邦政府的措施应当考虑以下三个战略要素：

（1）优化和明晰联邦政府各部门间的职能关系，使联邦加强关键基础设施的安全和韧性的工作具有一致性。

（2）明确基线数据和系统要求，使联邦政府能够有效地实现信息交换。

（3）实现整合和分析功能，使关键基础设施的规划和运行决策能够得到周知。

所有联邦各部、局负责人都对其各自的内部基础设施的标识、排列优先级、评估、修复和

安全负责，以支持该部、局的主要使命功能。这种基础设施应当在《国家连续性政策》的规划和实施中予以考虑。

联邦各部、局在执行本令时应当符合可适用的法律、总统令以及联邦法规，包括隐私保护、公民权利和公民自由等方面。此外，联邦各部、局应当遵循可适用的法律和政策，在执行本令时保护所有相关信息。

### 3. 角色和职责

有效地执行本令需要来自国土安全部长战略指导下的国家级一致努力。这种国家级的努力必须包括专业知识和日常参与，涉及关键基础设施对口机构（SSA）以及来自其他联邦各部、局的专业化或支撑性组织，还需要关键基础设施所有者和运营者及 SLTT 实体的强有力合作。虽然本令明确的角色和职责都是针对联邦部、局的，但对加强国家关键基础设施的安全和韧性而言，与关键基础设施所有者和运营者以及 SLTT 实体的有效合作是必不可少的。

#### 国土安全部长

国土安全部长应提供战略指导，促进整个国家一致、协调地去提高国家关键基础设施的安全和韧性。在执行 2002 年《国土安全法》修正案指定的职责时，国土安全部长评估了在保护关键基础设施时的国家能力、机会和挑战；分析了关键基础设施面临的威胁、脆弱性和所有危害的潜在后果；明确了与安全和韧性有关的功能，这对公共-私营部门有效地参与到各类关键基础设施行业中去十分必要；经咨商各对口部门（SSA）和其他关键基础设施合作伙伴，制定了一个国家计划和衡量标准；整合和协调了联邦的跨部门安全与韧性活动；标识并分析了各关键基础设施部门之间的互依赖性；报告了在强化国家安全及关键基础设施安全与韧性态势方面，国家所实施的一系列努力的有效性。

国土安全部长的其他角色和责任包括：

（1）经咨商各对口部门（SSA）和其他联邦部、局，标识关键基础设施并排列优先级，要考虑到物理和网络威胁、脆弱性以及后果。

（2）维护国家关键基础设施中心，该中心应提供态势感知能力，包括经整合的、可以指导行动的信息，涉及有关新趋势、迫在眉睫的威胁、可能影响关键基础设施的事件状态等。

（3）经与各对口部门（SSA）和其他联邦部、局协调，为关键基础设施所有者和运营者提供分析结果、专业知识和其他技术援助，便于获得对加强关键基础设施安全和韧性而言十分必要的信息和情报，以及加强这些信息和情报的交流。

（4）经咨商各对口部门（SSA），并与 SLTT 实体以及关键基础设施所有者和运营者开展合作，全面评估国家关键基础设施的脆弱性。

（5）根据法定授权，对联邦政府响应关键基础设施遇到的重大物理或网络事件进行响应。

（6）支持司法部长和执法机构，对关键基础设施的威胁和攻击进行调查和起诉。

（7）经与各对口部门（SSA）和其他适当的联邦部、局相协调，并利用其专业知识，通过采用商业卫星和机载系统以及其他部、局现有的能力，对关键基础设施进行地理的勘察、画像、分析以及分类。

（8）按照法规要求，每年报告国家关键基础设施的状况。

### 关键基础设施部门对口机构（SSA）

每个关键基础设施部门都有独有的特征、运行模式和风险场景，对联邦政府中已确定的对口机构而言，其对各自对口的关键基础设施有着体制上的知识和专业经验，对上述特征很熟悉。鉴于现有的法律法规已经对具体的联邦部、局进行了授权，而且为了充分利用这些联邦部、局对相应关键基础设施部门的熟悉程度及已建立的联系，各 SSA 应在各自相应的关键基础设施领域履行以下角色和职责：

（1）作为加强关键基础设施安全和韧性的更广泛的国家努力的一个组成部分，与国土安全部（DHS）和其他相关联邦部、局相协调，并与关键基础设施所有者和运营者相合作，且在必要时与独立的监管机构和 SLTT 实体相合作，以实施本令。

（2）针对优先级动态调整、协调对口关键基础设施有关的活动等事项，担当日常的接口。

（3）按照法定授权和其他适当的政策、指令或规定，履行事件管理责任。

（4）为对口的关键基础设施部门提供支持、技术协助和咨询，以标识脆弱性并在必要时协助减轻事件的影响。

（5）每年定期提供各关键基础设施部门的信息，为国土安全部长落实法定的报告要求提供支持。

### 其他联邦机构的责任

还有些与关键基础设施安全和韧性相关的特殊职能或支持性职能，需要其他部、局和独立的监管机构来实施，包括以下内容：

（1）经与 DHS、SSA 以及其他联邦部、局协调，国务院应与外国政府和国际组织合作，增强位于美国以外的关键基础设施的安全和韧性，全面加强对于最佳实践措施和经验教训的信息交流，以促进国家所依赖的关键基础设施的安全和韧性。

（2）司法部（DOJ），包括联邦调查局（FBI），将在关键基础设施部门中领导反恐和反情报调查及相关的执法活动。司法部应对国家关键基础设施面临的外部情报组织、恐怖分子和其他威胁，以及预谋或实际的对国家关键基础设施开展的攻击进行调查、阻断、起诉和其他处置。联邦调查局要在国内开展网络威胁信息的收集、分析和传播，并负责国家网络调查联合任务组（NCIJTF）的运行。NCIJTF 是一个负责协调、整合和分享与网络威胁调查信息的多部门的国家协调中心，与 DHS、情报共同体（IC）、国防部（DoD）和其他适宜机构的代表开展合作。司法部长和国土安全部长应合作实施各自的关键基础设施相关任务。

（3）经与关键基础设施部门中的“政府设施”部门对应的 SSA 合作，内政部应当针对国家纪念物和标志物的安全和韧性工作，开展标识、排列优先级和协调工作，采取措施降低这些关键资产的风险，同时提高其使用度和使用体验。

（4）经与 DHS 及其他有关联邦部、局合作，商务部（DOC）应吸引私营部门、研究机构、学术机构和政府机构的参与，提高网络系统相关技术和工具的安全性，并促进有关工作的开展，使国土安全所需的工业产品、材料和服务能实时可用。

（5）在国家情报总监领导下，情报共同体（IC）应利用适宜的权限和协调机制酌情实施关键基础设施威胁情报评估，并对涉及关键基础设施的情报和其他敏感信息、专属信息进行协调。另外，用于保护国家安全系统的信息安全政策、指令、标准和指南应受总统有关指示、可适用的法律所监督，与总统的指示相一致，并由该国家安全系统运营或使用单位的负责人授权后实施。

(6) 经与国防部、海关和其他部、局咨商，总务管理局（GSA）应为政府范围内的关键基础设施提供合同模板，并予以支持，确保这些合同中包含了对关键基础设施的安全和韧性的审计权。

(7) 核监管委员会（NRC）负责监督其许可证持有者对商业核反应堆和用于研究、测试和培训的非电力核反应堆的保护；监督在医疗、工业和学术环境中的核材料和制造核燃料的设施的保护；监督核材料及废料的运输、储存和处置过程中的保护。NRC 将在最大范围内与 DHS、DOJ、能源部、环境保护局以及其他联邦部、局合作，增强关键基础设施安全和韧性。

(8) 联邦通信委员会（FCC）将在法律允许的范围内行使其监督权力，提供专门知识，并与 DHS、国务院以及其他联邦部、局及 SSA 在以下方面合作：(a) 标识通信基础设施并排列其优先级；(b) 查找通信部门的脆弱性，并与产业界及其他利益相关方合作解决这些脆弱性；(c) 与包括产业界在内的利益相关方合作，吸引外国政府和国际组织参与，提高通信部门关键基础设施的安全和韧性，推动制定和实施有助于提高国家所依赖的关键通信基础设施安全和韧性的最佳实践措施。

(9) 联邦各部、局应及时向国土安全部长和国家关键基础设施中心提供信息，以支持跨关键基础设施部门的分析，并向关键基础设施提供态势感知能力。

## 4. 三个战略要求

(1) 优化和明晰联邦政府各部门间的职能关系，使联邦加强关键基础设施的安全和韧性的工作具有一致性

一个有效的增强关键基础设施安全和韧性的国家级行动必须以国家计划为指导，这个国家计划要明确角色和职责，在其中要体现各个 SSA、其他担负关键基础设施角色的联邦各部、局以及 SLTT 实体、关键基础设施所有者和运营者的专业知识、经验、能力和职责。

在过去 10 年中，针对特定基础设施问题的新项目和新举措已经建立起来，优先事项也已发生转移和延伸。因此，与关键基础设施安全和韧性有关的联邦职能应进一步明晰和优化，以形成基础能力，从而反映出知识的变化。还要界定联邦相关工作的职能，促进联邦政府、关键基础设施所有者和运营者以及 SLTT 实体之间的合作与信息交流。

作为这一优化的体系结构的一部分，应由 DHS 运营两个国家关键基础设施中心，一个用于物理基础设施，另一个用于网络基础设施。它们将以整合的方式运行，并作为关键基础设施合作伙伴的中心点，能够获得态势感知及综合、可指导行动的信息，以保护关键基础设施的物理和网络部分。正如关键基础设施的物理和网络部分是不可避免的、互相关联的，脆弱性也是如此。因此，在这两个国家中心之间应实现一体化和分析功能（在后文的战略任务 3 中进一步提出要求）。

这些国家中心的成功，包括整合和分析功能，取决于它们从 SSA 和其他联邦部、局以及关键基础设施所有者和运营者、SLTT 实体获得的信息和情报的质量和及时性。

这些国家中心不得妨碍联邦各部、局负责人执行或履行国防、刑事、反情报、反恐或调查活动的职责。

(2) 明确基线数据和系统要求，使联邦政府能够有效地实现信息交换

一个安全、可靠和富有韧性的关键基础设施需要在各级政府和关键基础设施所有者及运营

者之间有效交流信息，包括情报。这就必须及时交换威胁和脆弱性信息以及形成态势感知能力所需的信息。目标是通过明确数据和信息的格式要求，以及明确信息可访问性、系统互操作性、冗余系统和备份能力等要求，提高信息交流的效率。

政府和私营部门之间的信息共享必须做到尊重隐私和公民自由。联邦各部、局应确保所有现行的隐私原则、政策和流程根据法律要求得到实施，还应在本机构高级隐私官的工作中加入对信息共享进行监督管理的内容。

(3) 实现整合和分析功能，使关键基础设施的规划和运行决策能够得到周知

本战略任务建立在前两个任务基础上，呼吁实现关键基础设施的整合和分析功能，包括对事件、威胁和新风险的运营级与战略级分析。其应位于战略任务（1）中确定的两个国家中心的交汇处，并应包括将脆弱性及事件后果信息与威胁信息进行整理、评估和整合的能力。

① 优先考虑关键基础设施资产并管理其风险。

② 预测互依赖性和级联影响。

③ 在事件发生之前、期间和之后，为关键基础设施推荐安全和韧性措施。

④ 支持与关键基础设施相关的事件管理和恢复工作。

该功能不可复制情报共同体或国家反恐中心的分析功能，也不会涉及情报收集活动。情报共同体、国防部、司法部、国土安全部及其他具有相关情报或信息收集的联邦部、局应向国家中心提供相关、及时、适宜的信息，以提升其针对国家关键基础设施的信息整合和分析能力。此功能还应利用其他关键基础设施合作伙伴，包括 SLTT 和非政府分析实体，提供的信息和情报。

最后，这种整合和分析功能应支持国土安全部维护和共享关键基础设施准实时态势感知的能力，包括可能面临的威胁、重大趋势等信息以及对可能影响关键基础设施的事件的感知，这是国土安全部自身的一种联邦公共服务。

## 5. 创新和研发

经与科技政策办公室（OSTP）、各 SSA、商务部和其他联邦部、局相协调，国土安全部长应提供有关信息，便于同联邦及联邦资助的旨在加强国家关键基础设施安全和韧性的研发（R & D）活动保持一致，包括：

(1) 促进研发，使关键基础设施得到安全和韧性的设计与建设，以及实现更安全的网络技术。

(2) 增强建模能力，以研判事件或威胁情景对关键基础设施的潜在影响，以及对其他关键基础设施部门的级联影响。

(3) 激励对网络安全的投资，促进关键基础设施采用有助于加强安全和韧性的设计特性。

(4) 优先支持国土安全部长发布的战略指导意见。

## 6. 指令的实施

国土安全部长应采取以下行动：

(1) 关键基础设施安全和韧性职能关系。在本令发布后的 120 天内，国土安全部长应对 DHS 内部及联邦政府中与关键基础设施安全和韧性有关的职能之间的关系进行描述。其中应包括两个国家关键基础设施中心的角色和职能，并对分析与整合职能进行讨论。这项工作完成后，



其应作为关键基础设施所有者、运营者以及 SLTT 实体的路线图，以引导联邦政府的职能和主要的联络点围绕关键基础设施安全和韧性做出分配，以抵御物理和网络威胁。部长应与各 SSA 和其他相关联邦部、局协调这一工作。部长还应通过总统国土安全和反恐助理向总统提供对这一职能关系的描述。

(2) 评估现有的公共-私营合作模型。在本令发布后的 150 天内，经与各 SSA、其他相关联邦部、局和 SLTT 实体、关键基础设施所有者和运营者相协调，国土安全部长应对现有的公共-私营合作模型进行分析并提出建议，以提高在物理和网络空间中合作关系的有效性。评估应考虑如何优化合作程序和信息交流程序的方案，以减少重复工作。此外，还应考虑如何使模型具有灵活性和适应性，从而既能满足各个关键基础设施部门的独特需求，也能为联邦政府同关键基础设施所有者和运营者以及 SLTT 政府进行协调而提供重点突出、成熟和有效的方法。完成评估后，要对如何提升公共-私营合作关系提出建议，以便通过《国家安全咨询系统组织指令》中确立的程序来批准和实施。

(3) 明确数据和系统的基线要求，使联邦政府能够实现高效的信息交换。在本令发布后的 180 天内，经与各 SSA、其他联邦部、局相协调，国土安全部长应召集一个专家小组，确定数据和系统的基线要求，便于高效地交换与加强关键基础设施安全和韧性有关的信息和情报。专家应包括来自以下实体的代表：持有对关键基础设施安全和韧性而言十分重要的信息的实体，决定和管理信息交换所需的 IT 系统的实体，以及负责所交换信息的安全的实体。在开展分析时，需要考虑以下因素：与关键基础设施合作伙伴的互操作性；关键的联邦实体、SLTT 和私营部门实体对数据和信息的需求；数据可用性、可访问性和格式；交换不同密级信息的能力；所用的那些系统的安全性；对个人隐私和公民自由应有的保护。分析工作完成后，应当生成一个数据共享的基线要求以及对系统互操作性的基准要求，以便及时交换数据和信息，确保关键基础设施的安全性，并使其更富有韧性。部长应通过总统国土安全和反恐助理向总统提供分析结论。

(4) 发展关键基础设施的态势感知能力。在本令发布后的 240 天内，国土安全部长应对关键基础设施展示准实时的态势感知能力，包括威胁和危险信息，以及脆弱性信息；应能提供与关键基础设施状态和可能的级联效应相关的信息；应支持决策；应发布有关关键信息，以拯救生命、减轻损害或防止关键基础设施能力因事件而进一步而恶化。这种能力应该可用于关键基础设施的所有物理和网络部分，并有助于在必要时实现信息整合。

(5) 更新国家基础设施保护计划。在本令发布后的 240 天内，国土安全部长应通过总统国土安全和反恐助理向总统提供新版的《国家基础设施保护计划》。该计划要落实本令的实施以及 2002《国土安全法》修正案第二章提出的要求，并符合 PPD-8 要求的“国家战备目标和系统”。在该计划中，要确定用于增强关键基础设施安全和韧性的风险管理框架；提出用于对关键基础设施进行优先级排序的方法；建立用于对联邦政府内的通信及行动进行同步的协议；描述用于衡量国家管理和降低关键基础设施风险的能力指标和分析流程。新版计划还应反映 DHS 内和整个联邦政府之间已确定的职能关系，以及新的公共-私营合作模型。最后，该计划还应考虑到各关键基础设施部门对能源和通信系统的依赖性，说明在遇到能源和通信系统中断时有哪些事前措施和缓解措施，或者有哪些替代性的功能。就此项工作，国土安全部长应与各 SSA、其他相关联邦部、局以及 SLTT 实体、关键基础设施所有者和运营者进行协调。

(6) 国家关键基础设施安全和韧性研发计划。在本令发布后的 2 年内，经与总统科技政策

办公室（OSTP）、各 SSA、商务部（DOC）和其他联邦部、局相协调，国土安全部长应通过总统国土安全和反恐助理向总统提交《国家关键基础设施安全和韧性研发计划》。该计划应考虑到不断变化的威胁场景、年度评价指标和其他相关信息，以确定研发优先事项，并指导研发需求及投资。该计划在初次发布后应每 4 年更新一次，必要时可进行临时更新。

本令实施中的政策协调、争议解决和定期审查应与 PPD-1 一致，包括动用由国家安全委员会协调下的机构间政策委员会。

本令中的任何内容都不会改变、取代或阻碍有关法律、其他的总统指南或总统令对联邦各部、局的授权，包括对独立监管机构的授权，也不会改变、取代或阻碍已有法律或总统指南、总统令中对关键基础设施的指定授权。

该令撤销了 2003 年 12 月 17 日发布的第 7 号国土安全总统指令（HSPD-7）《关键基础设施标识、优先级和保护》。根据 HSPD-7 制定的计划将一直有效，除非被特别撤销或取代。

## 7. 指定的关键基础设施部门和对口机构

该令确定了 16 个关键基础设施部门，并指定了相关联的联邦对口机构（SSA）。在某些情况下，有时要共同指定 SSA，因为这些部门分担着共同的角色和职责。国土安全部长应定期评估是否需要变更关键基础设施部门清单或 SSA，并对新的变更予以批准。但在变更前，应同总统国土安全和反恐助理相协商。关键基础设施部门和对口的 SSA 如下：

### 化学

对口机构：国土安全部。

### 商业设施

对口机构：国土安全部。

### 通信

对口机构：国土安全部。

### 关键制造业

对口机构：国土安全部。

### 大坝

对口机构：国土安全部。

### 国防工业基地

对口机构：国防部。

### 应急服务

对口机构：国土安全部。

### 能源

对口机构：能源部。

### 金融服务

对口机构：财政部。

### 食品和农业

联合对口机构：美国农业部和健康与公众服务部。

### **政府设施**

联合对口机构：国土安全部和总务管理局。

### **健康和公共卫生**

对口机构：健康与公众服务部。

### **信息技术**

对口机构：国土安全部。

### **核反应堆、材料和废料**

对口机构：国土安全部。

### **交通系统**

联合对口机构：国土安全部和交通部。

### **供水和废水系统**

对口机构：环境保护局。

## **8. 定义**

在本令中，相关术语定义如下：

“所有危害”指自然或人为的威胁或事件，为此需要采取行动去保护生命、财产、环境和公共卫生或安全，并最大可能地减少对政府、社会或经济活动的破坏。其包括针对关键基础设施的自然灾害、网络事件、工业事故、大流行病、恐怖主义行为、大破坏以及破坏性犯罪活动。

“合作”指共同努力实现共同目标的过程。

“协调”和“与……协调”指一种得到共识的决策过程，通过这一过程，指定的协调部、局要同受影响的部、局合作，达成共识和一致的行动路线。

“关键基础设施”为在 2001 年《美国爱国者法》（《美国法典》第 42 编第 5195c（e）章）的第 1016（e）节定义，即物理或虚拟的系统和资产，它们对美国至关重要，因为这些系统和资产一旦失去运转能力或遭到破坏，会对国家安全、国家经济安全、国家公共健康和安全的一个或多个方面造成破坏性影响。

“联邦部、局”是指除了那些被考虑作为独立监管机构（《美国法典》第 44 编第 3502（2）节定义）的单位外，在《美国法典》第 44 编第 3502（1）节中定义的“机构”。

“国家基本职能”是指在灾难性的突发事件下，领导和维持国家运转所需的政府职能。

“主要任务重要职能”是指在紧急情况之前、期间和之后，为了支持或实现国家基本职能的实施，必须执行的政府职能。

“国家安全系统”在 2002 年《联邦信息安全管理法》（《美国法典》第 44 编第 3542（b）节）中进行了定义。

“韧性”是指为不断变化的条件做好准备并去适应，能承受破坏且可从中迅速恢复的能力。韧性包括能够经受故意攻击、事故或自然发生的威胁或事件，并从中恢复的能力。

“部门对口机构”（SSA）在本令中是指有关的联邦部、局，其可在各类威胁环境中，为指定的关键基础设施部门提供体制上的知识和专业经验，并领导、推动和支持安全、韧性工作及相关活动。

“安全的”和“安全”是指通过物理手段或防御性的网络措施减少关键基础设施风险，应对入侵、攻击以及自然或人为灾害的影响。

---

## 二十四、第 13636 号行政令：增强关键基础设施网络安全

美国白宫

2013 年 2 月

---

作为总统，利用美国宪法和法律赋予我的权力，现命令如下：

## 1. 政策

不断针对关键基础设施的网络入侵凸显了提高网络安全的必要性。关键基础设施受到的网络威胁呈逐年上升之势，这是我们面临最严重的国家安全挑战之一。美国国家和经济安全依赖于关键基础设施在面临威胁情况下可靠的运行。为提高国家关键基础设施的安全性、恢复力，维护网络空间，美国的政策原则上鼓励高效、创新和经济发展，促进安全、商业秘密、隐私和公民自由。通过与关键基础设施所有者及运营者的密切合作，增加网络安全信息共享，联合开发并实施基于风险的标准。

## 2. 关键基础设施

本令中，关键基础设施是指对美国极为重要的系统和资产，不论物理的或虚拟的，其遭到破坏或失去运转能力时，将对美国国家安全、经济安全、公共健康或安全中的一项或多项产生破坏性影响。

## 3. 政策协调

本令所描述、指定的职能和计划，包括政策协调、指导、争端解决和周期性进展审查等，应由 2009 年 2 月 13 日发布的 1 号总统政策指示（国家安全委员会体系内的组织）或后续文件确立的跨部门流程实施。

## 4. 网络安全信息共享

(a) 美国政府的政策是与美国私营部门实体在数量、及时性和质量上增加网络威胁信息共享，促使这些实体更好地抵御网络威胁。自本令公布之日起 120 天内，司法部长、国土安全部长（以下简称“部长”）以及国家情报总监应根据各自职权和本令第 12 (c) 条的要求发布指令，确保及时发布有关美国本土网络威胁非涉密报告，指令中要确定具体目标实体。指令应满足保护情报和执法资源、方法、操作和调查的需求。

(b) 部长、司法部长和国家情报总监应依据本令第 4 (a) 条建立相应流程，向目标实体迅速发送报告。该流程也应遵循保护国家安全信息的原则，包括向授权关键基础设施实体发送涉密报告。部长、司法部长和国家情报总监应建立相应系统，用于跟踪该类报告的产生、传播和处置。

(c) 为了协助关键基础设施的所有者和运营者，保护其系统遭受未授权的访问、利用和破坏，部长应遵循《美国法典》第 6 编第 143 节的规定并与国防部部长合作，自本令公布之日起 120 天内，建立起一套将“增强型网络安全服务方案”扩展到所有关键基础设施部门的程序。这种自愿信息共享计划将向符合条件的关键基础设施企业或承担关键基础设施安全服务的商

业服务供应商，提供政府的涉密网络威胁和技术信息。

(d) 部长作为 2010 年 8 月 18 日实施的 13549 号行政令《涉密国家安全信息计划》（即面向州、地方、部落和私营部门实体的涉密国家安全信息计划）的执行机构，应加快处理关键基础设施所有者和运营者中合适雇员的安全审查，这项工作中应优先考虑本行政令第 9 节中识别的关键基础设施。

(e) 为最大程度地发挥与私营部门共享网络威胁信息的效果，部长应扩大计划执行范围，使私营部门主题专家能够临时性地进入联邦服务。这些主题专家应就信息的内容、结构和类型，向关键基础设施所有者和运营者提出最有价值的意见，以减少和减轻网络风险。

## 5. 隐私和公民自由保护

(a) 依据本令，各机构应与其机构中负责隐私和公民自由的高级官员相协调，确保将隐私和公民自由保护纳入其中。这应以“公平信息实践原则”以及其他隐私和公民自由政策、原则和框架为基础。

(b) 国土安全部首席隐私官员、公民权利和公民自由官员应根据本令要求，评估国土安全部职能和计划中有关隐私和公民自由的风险，以公开报告形式向部长推荐减少或减轻风险的方法，并在本令公布 1 年之内发布。其他机构的高级隐私和公民自由官员在参与本令下的活动时，应评估该机构活动，并将评估结果报送国土安全部。此报告应进行年度审查，必要时进行修订。如果需要，报告可包含涉密附件。评估结果应以“公平信息实践原则”、其他隐私和公民自由政策、原则和框架等为依据。各机构在开展本机构的隐私和公民自由保护时，应考虑报告中的评估结果和建议。

(c) 按照本节 (b) 条要求，在完成报告时，国土安全部首席隐私官员、公民权利和公民自由官员应与隐私和公民自由监督委员会协商，并与行政管理和预算办公室协调。

(d) 根据本令，按照《美国法典》第 6 编第 133 节的规定，由私营实体自愿提交的信息应在最大程度上受到法律保护不被公开。

## 6. 咨询过程

部长应建立咨询程序，以协调关键基础设施网络安全保障。作为咨询程序的一部分，在本令提出的事项上，部长应吸收并考虑关键基础设施合作咨询委员会、行业协调委员会、关键基础设施所有者和运营者、各行业的对口政府机构、其他相关机构、独立监管机构、州和地方及部落政府、大学和外部专家的建议。

## 7. 减少关键基础设施网络风险的基本框架

(a) 美国商务部部长应该指导国家标准与技术研究院 (NIST) 主任(以下简称“主任”)，领导制定一项旨在降低关键基础设施网络风险的网络安全框架。网络安全框架应包括一系列标准、方法、程序和流程，结合政策、业务和技术方法来应对网络风险。网络安全框架应最大程

度地纳入自愿、一致标准和产业最佳实践。当有国际标准能够有助于实现本令目标时，网络安全框架应与自愿性的国际标准相一致。同时，框架应符合《国家标准与技术研究院法》（经修订），1995 年《国家技术转移与促进法》和行政管理和预算办公室通告（A-119）（经修订）的要求。

（b）网络安全框架应提供最优先的、灵活的、可重复的、基于绩效管理和成本有效的方法，包括信息安全措施和控制，协助关键基础设施的所有者和运营者识别、评估和管理网络风险。网络安全框架应重点关注识别关键基础设施的跨部门安全标准和指南。未来，通过与具体的行业 and 标准开发组织的合作，网络安全框架还将明确改进之处。为了保持技术创新和维护组织间的差异，网络安全框架将提供中立的技术指导，确保关键基础设施部门通过竞争性的产品和服务市场受益，这些产品和服务都将符合网络安全风险标准、方法、程序和流程。在实施过程中，网络安全框架应包括衡量实体绩效的指南。

（c）网络安全框架应包括识别和减轻威胁造成影响的方法，以及商业秘密等相关的信息安全措施或控制，并保护个人隐私和公民自由。

（d）在制定网络安全框架过程中，主任应有一个公开审查和征求意见的程序。利用本令第 6 节建立的咨询过程，主任也应向部长、国家安全局、各行业的对口政府机构以及行政管理和预算办公室等其他政府机构、关键基础设施所有者和运营者以及其他利益相关者进行咨询。部长、国家情报总监和其他相关机构负责人应提供威胁和漏洞信息以及专业技术，促进网络安全框架发展。根据本令第 9 节的工作，部长应为网络安全框架提供设计绩效目标。

（e）自本令公布之日起 240 天内，主任应发布网络安全框架初始版（初始框架）。自本令公布之日起 1 年内，根据本令第 8 节，在与部长协调以确保适用性后，主任应发布网络安全框架最终版（最终框架）。

（f）考虑到技术变革、网络风险变化、关键基础设施所有者和运营者的操作反馈、本令第 8 节的实施经验和其他相关因素，主管将遵循法定责任，在必要时对网络安全框架和相关指南进行审查和更新。

## 8. 自愿性关键基础设施网络安全项目

（a）部长应与各行业的对口政府机构协调，建立一项自愿性的项目，支持关键基础设施所有者或运营者以及其他相关实体采用本令所述网络安全框架（以下简称“项目”）。

（b）经咨询部长和其他相关机构，各行业的对口政府机构应协调各自行业的协调委员会，以审查网络安全框架，必要时制定实施指南或补充材料，以适应具体行业风险和操作环境。

（c）各行业的对口政府机构每年应通过部长向总统提交报告，说明本令第 9 节公布的关键基础设施所有者和运营者参与项目的程度。

（d）部长应协调建立一套促进本项目参与度的激励措施。自本令公布之日起 120 天内，国土安全部长、财政部长和商务部长应通过总统国土安全和反恐事务助理、总统经济事务助理分别向总统提出建议，分析这些激励措施的优点、相对有效性，以及激励措施是否需要立法或现有法律和授权已经可以提供。

（e）自本令公布之日起 120 天内，国防部长和总务管理局长应向部长和联邦采购监督管理委员会咨询，通过总统国土安全和反恐事务助理以及总统经济事务助理向总统提出建议，阐述

在采购计划和合同管理中引入安全标准的可行性、安全好处和优缺点。该报告应说明采用何种措施协调，以保持与现有网络安全相关采购要求相一致。

## 9. 标识处于最大风险的关键基础设施

(a) 自本令公布之日起 150 天内，部长应使用基于风险的方法，标识那些一旦发生网络安全事件便有可能在地区或全国范围内对公众健康或安全、经济安全、国家安全造成灾难性影响的关键基础设施。在这项工作中，部长应利用本令第 6 节建立的咨询程序，并结合各行业的对口政府机构的专业知识。部长应采用一致的、客观的标准来识别这些关键基础设施。在此节中，部长不应标识任何商用信息技术产品或消费类信息技术服务。部长应每年修订、更新本节所标识的关键基础设施列表，并通过总统国土安全和反恐事务助理、总统经济事务助理，将列表提交给总统。

(b) 各行业的对口政府机构和其他相关政府机构的主管，应向部长提供落实本节任务的必要信息。部长应为其他利益相关者制定流程，以使其能够提交信息，帮助做好这项工作。

(c) 部长应与各行业的对口政府机构相协调，以保密方式通知本节 (a) 条中被标识的关键基础设施所有者和运营者，并向所有者和运营者提供做出该决定的依据。部长应制定建立相应流程，通过该流程，关键基础设施的所有者和运营者可提交相关信息，并请求部长重新考虑是否将其设施列入根据本节 (a) 条的列表中。

## 10. 框架的采用

(a) 关键基础设施安全监管机构，应参与到咨询过程之中，与国土安全部、行政管理和预算办公室以及国家安全工作班子沟通，审查初始的网络安全框架，判断当前网络安全监管要求是否足以应对当前及预计的风险。在做判断时，这些机构应将本令第 9 节所标识的关键基础设施作为考虑对象。在网络安全初始框架公布之日起 90 天内，这些机构应通过总统国土安全和反恐事务助理、行政管理和预算办公室主任以及总统经济事务助理，向总统提交一份报告，说明该机构是否有明确的授权，能够建立以网络安全框架为基础的监管要求来应对当前和预计的关键基础设施安全风险，以及现有的授权和还需补充的授权。

(b) 如果当前的监管要求不充分，最终框架公布之日起 90 天内，本节 (a) 条指出的机构应提出应优先实施的、基于风险的、高效并可协调的行动方案，并遵循 1993 年 9 月 30 日第 12866 号行政令《监管规划和审查》、2011 年 1 月 18 日第 13563 号行政令《改善法规和监管审查》和 2012 年 5 月 1 日第 13609 号行政令《促进国际监管合作》，以减少网络风险。

(c) 最终框架公布两年内，本节 (a) 条指出的机构应遵循 2012 年 5 月 10 日第 13563 号行政令和 2012 年 5 月 10 日第 13610 号行政令《确认和降低监管负担》，并经咨询关键基础设施的所有者和运营者，向行政管理和预算办公室报告有关关键基础设施遇到无效、冲突和负担过分的网络安全要求的情况。该报告应说明各机构为此所做的努力，并针对下一步行动提出建议，以减少或消除此类要求。

(d) 部长应协调对本节 (a) 条中所指出的各机构在网络安全队伍建设和工作开展等方面提供的技术支持。



(e) 鼓励各个负有关键基础设施安全监管职责的独立监管机构，在咨询过程中同部长、各行业的对口政府机构和其他相关方相协商，以考虑最应优先采取的活动，以在其职权下降低关键基础设施的网络风险。

## 11. 定义

(a) “机构”指《美国法典》第 44 编 3502 节第 (1) 条中任何美国政府当局，《美国法典》第 44 编 3502 节第 (5) 条所定义的独立管理机构除外。

(b) “关键基础设施合作咨询委员会”指国土安全部依据《美国法典》第 6 编第 451 节定义的委员会，以促进联邦政府、私营部门、各州、地方、区和部落政府的关键基础设施保护活动的有效互动性和协调性。

(c) “公平信息实践原则”指《网络空间可信身份国家战略》附录 A 中的八项原则。

(d) “独立监管机构”参照《美国法典》第 44 编 3502 节第 (5) 条中的术语。

(e) “行业协调委员会”指私营行业协调委员会，该委员会由关键基础设施的所有者和运营者代表组成，国家基础设施保护计划或后续文件确定的具体行业中，每个行业都有一个协调委员会。

(f) “行业的对口政府机构”参照 2013 年 2 月 12 日第 21 号总统政策令《关键基础设施的安全性和恢复力》或后续文件给出的阐述。

## 12. 总则

(a) 本令应在遵循适用法律和服从可用预算的情况下实施。现有法律体系下，在关键基础设施安全方面，本令任何内容不可赋予某个机构超出其职权更广范围的权利。在现有法律体系下，本令中任何内容都不可改变或限制某个机构的任何职权或责任。

(b) 本令中任何内容，不得妨碍或以其他方式影响行政管理和预算办公室主任的职能，包括财政预算、行政或立法建议。

(c) 本令施行的所有活动应遵循保护情报和执法资源及方法的要求与授权。本令中任何内容都不可取代在法律授权下建立的安全和完整性措施，以保护情报和执法行动中的具体活动和关联信息。

(d) 本令的施行应符合美国的国际义务。

(e) 本令不拟，也不会创设可被任何派别对美国及其各部、局、实体、其官员、雇员或代理以及任何其他要求实施的权利或利益，无论是在实体法还是程序法上，也无论是在普通法还是衡平法上。

——奥巴马

---

## 二十五、增强关键基础设施网络安全框架 (CSF)

美国国家标准与技术研究院 (NIST)

2014 年 2 月

---

## 执行摘要

美国的国家安全与经济安全依赖于关键基础设施的平稳运行。网络安全威胁利用关键基础设施系统日益增长的复杂性和关联性，将国家安全、经济及公共安全与健康置于危险之中。同样，网络安全风险也会给企业带来影响，提高企业成本并影响收益，损害企业改革创新的能力以及获取并维护客户的能力。

为了更好地应对风险，总统于 2013 年 2 月 12 日颁布了第 13636 号行政令《增强关键基础设施网络安全》。该行政令明确指出：“该政策旨在增强国家关键基础设施的安全和韧性，构建一个鼓励高效、创新和经济繁荣的网络环境，同时促进安全、商业秘密、隐私和公民自由。”为了实施这一政策，该行政令要求制定一个自愿实施的网络安全框架以确定产业标准与最佳实践，帮助组织管理网络安全风险。本框架由政府与私营部门共同协作完成，采用通用语言阐述了如何基于成本效益方式应对网络安全风险，而不对企业提出额外的合规要求。

本框架强调利用业务驱动指导网络安全行动，将网络安全风险作为组织风险管理程序的一部分。

本框架包含三部分内容：框架核心、框架轮廓和框架实施层级。框架核心是一套关键基础设施部门通用的网络安全行动、预期成果和参考文献，为组织开发各自的安全框架提供了详细的指南。通过使用轮廓，本框架可帮助组织把网络安全行动及业务需求、风险承受力和资源结合起来。框架实施层级为组织提供了一种机制，使组织可以查看和了解其管理网络安全风险的特点。

行政令还要求，在关键基础设施组织实施网络安全行动时，框架还要包括保护个人隐私和公民自由的方法。如果程序和现实需求有分歧，那么本框架可帮助组织将保护隐私和公民自由合并到综合网络安全计划中。

无论关键基础设施组织规模大小、网络安全风险程度高低、网络安全形势复杂程度，本框架都能提供风险管理原则和最佳实践，提升关键基础设施的安全和韧性。本框架提供了当前产业界最有效的标准、指南和实践。此外，本框架采用全球认可的网络安全标准，因此适用于美国之外的组织，可作为增强关键基础设施网络安全国际合作的模板。

本框架不是一个放之四海而皆准的关键基础设施网络安全管理方法，因为各类组织面临的威胁和脆弱性不同，拥有的风险承受力不同，它们如何执行框架的相关措施也会有所不同。各组织可以根据关键交付服务的重要性决定所采取的行动，也可以根据投资收益优先级采取不同措施。本框架的主旨是减少和更好地管理网络安全风险。

本框架是一份动态文件，将根据产业在实践中提供的反馈持续更新和优化。在实际操作中，本框架会不断吸取经验教训，并融合到框架的新版本中，以确保本框架在一个具有新威胁、新风险和解决方案，且充满挑战的新环境中，满足关键基础设施所有者和运营者的需求。

利用好该自愿性网络安全框架可提升我国关键基础设施的网络安全，一方面改善国家关键基础设施网络安全态势，另一方面为每个人组织提供指南。

## 1. 框架介绍

美国的国家安全与经济安全依赖关键基础设施的平稳运行。为增强关键基础设施的韧性，奥巴马总统于 2013 年 2 月 12 日签署了第 13636 号行政令《增强关键基础设施网络安全》。该令要求制定一个自愿实施的网络安全框架，旨在提供一个“具有优先级的、灵活的、可重复使用的、成本效益比高的方法”来管理关键基础设施的网络安全风险。这个由产业界参与制定的安全框架可为组织的网络安全风险管理提供指南。

关键基础设施在行政令中的定义：对美国极为重要的系统和资产，不论物理的或虚拟的，其遭到破坏或失去运转能力时，将对美国国家安全、经济安全、公共健康或安全中的一个或多个方面产生破坏性影响。由于来自内部和外部威胁的压力不断增加，负责关键基础设施的组织需要有一套持续的、可重复使用的方法来识别、评估和管理网络安全风险。不论组织的规模、所面临的威胁或网络安全的复杂程度如何，这个方法都是必要的。

关键基础设施团体包括拥有和运营关键基础设施的公共-私营部门以及负责安全的其他部门。每个关键基础设施部门的运行都基于信息技术（IT）和工业控制系统（ICS）的支持。组织对技术、通信和工业控制系统的依赖改变和扩大了可能的脆弱性，增加了运行中的潜在风险。例如，工业控制系统以及在工业控制系统操作中产生的数据越来越多地用于提供关键服务和支持业务决策，该情况下，应当考虑安全事件对于一个组织的业务、资产、个人健康和安全以及环境方面的潜在影响。为了管理网络安全风险，有必要清楚地了解机构的驱动力，以及在信息技术和工业控制系统中的安全考虑。不同组织机构利用的信息技术和工业控制系统不同，面临的网络安全风险各异，因此为实现本框架描述的结果所用的工具和方法也会有所不同。

考虑到保护隐私和公民自由在建立公共信任中发挥的作用，行政令要求框架包含一套开展网络安全活动时保护个人隐私和公民自由的方法。很多组织已制定了保护隐私和公民自由的程序。设计这套方法是对组织程序的补充和提供指南，使隐私风险管理与网络安全风险管理保持一致。将隐私和网络安全统一起来可提升客户信心，促进标准化的信息共享，简化法律操作程序，从而使组织机构获益。

为了确保可扩展性和便于技术创新，本框架保持技术中立原则。框架基于现有标准、指南、实践，以确保关键基础设施运营商具有韧性。依托业界制定的全球标准、指南、实践，框架中的工具和方法将超越国界，体现网络安全风险的全球性，并随着技术进步和企业需求进行持续改进。使用现有和新兴标准有利于实现规模经济，促进开发符合市场需求的高效产品、服务和实践。市场竞争也会促进这些技术和实践的快速传播，使这些部门的利益相关方受益。

基于这些标准、指南和实践，本框架为组织机构提供了一个通用的分类方法和机制，以便：

- （1）描述当前网络安全形势；
- （2）描述网络安全目标状态；
- （3）确认改进的机会并明确优先级；
- （4）评估为达到目标状态所取得的进展；
- （5）就网络安全风险与内部和外部利益相关方沟通。

框架对于组织的风险管理程序和网络安全计划来说是一个补充，而非替换。各组织可以使用其当前的管理办法并利用框架来确认其改善网络安全风险管理的机会。若组织没有网络安全

计划，则可以框架为参考制定一个网络安全计划。

本框架并不囿于某一特定行业，它对于标准、指南与实践的通用分类方法也并非针对某一特定国家。海外组织也可使用本框架加强其网络安全管理，相关国际合作亦可参考框架制定统一标准。

### 框架概述

本框架是一个用于管理网络安全风险的方法，包含三个部分：框架核心、框架实施层级和框架轮廓，每部分都强调业务驱动与网络安全活动之间的联系，具体如下。

（1）框架核心：是一系列关键基础设施部门公认的网络行动、理想结果和可用参考。框架核心提供了产业网络安全标准、指南和最佳实践，组织可基于此对网络安全活动与结果在组织内部上传和下达。框架核心包括五个并行且连续的功能：识别、防护、检测、响应、恢复。这些功能作为一个整体，可为组织网络安全风险管理提供高层次的战略视角。框架核心还确定了各功能的关键类和子类，以及相应的参考资料，如标准、指南和实践。

（2）框架实施层级：为组织提供了评估网络安全风险的背景以及针对此种风险的现有管理流程。层级描述了组织的网络安全风险管理活动与框架所定义特点的符合程度。层级从部分实施（1级）至自适应（4级）。该层级分类反映了从非正式、被动的响应层级到迅速的、基于可靠风险信息的响应层级。在层级选择过程中，各组织应考虑其现有的风险管理实践、威胁环境、法律规范、业务/任务目标和组织局限性。

（3）框架轮廓：描述了与业务需求相匹配的结果，这些业务需求由组织根据框架定义的和子类进行选择。轮廓可被视为在实际场景下框架核心与标准、指南和实践的对齐。通过对比当前轮廓和目标轮廓，确认提升网络安全态势的机会。在建立轮廓时，组织需要评估所有的类和子类，然后根据业务驱动和风险评估，确定哪个更为重要。当前轮廓支持优先级排序，衡量目标轮廓的进展，同时考虑成本效率与创新等业务需求。框架轮廓适用于自我评估以及组织内和跨组织的沟通。

### 风险管理和网络安全框架

风险管理是风险识别、评估和响应的持续过程。为了更好地管理风险，组织应了解事情发生的可能性以及可能导致的影响。利用这些信息，组织可以确定交付服务时可接受的风险级别，即组织的风险承受能力。

组织根据风险承受能力确定网络安全活动的优先级，并对网络安全支出做出明智的决策。组织可通过实施风险管理计划来量化自身网络安全计划变化，并可根据关键服务交付的潜在影响采用不同方法处理风险，如减轻风险、转移风险、规避风险或接受风险。

组织可利用本框架提供的风险管理流程传达与网络安全相关的决策并确定其优先级。本框架支持重复性风险评估、业务驱动认定，帮助组织确定网络安全活动的目标状态。因此，本框架可帮助一个组织选择并改善信息技术（IT）和工业控制系统（ICS）环境的网络安全风险管理。

框架提供了灵活的、基于风险的实施策略，适用于各类网络安全风险管理流程，如（ISO）31000:2009、ISO/IEC 27005:2011、NIST SP800-39、《电力行业网络安全风险管理程序指南》等。

### 文档总览

本文档的后续内容如下。

- 第二部分描述了框架构成。包括框架核心、框架实施层级和框架轮廓。

- 第三部分列举了框架应用的例子。
- 附录 A 以表格形式列出了框架的核心：功能、类、子类以及参考资料<sup>①</sup>。
- 附录 B 列出了一些术语。
- 附录 C 列出了文档出现的缩略语。

2. 框架基本要素

本框架为理解、管理、表述内部和外部的网络安全风险提供了通用的语言。其有助于确定可降低网络安全风险的活动并定义其优先级，还可调整风险管理策略、业务和技术方法。框架既可用来管理整个组织的网络安全风险，也可集中处理组织内部的关键服务交付，还可协调机构、协会、组织在内的各类团体根据不同的目的使用本框架，包括创建通用的轮廓。

框架核心

本框架核心提供了一系列为实现特定网络安全目标而开展的行动及指导示例作为参考。框架核心不是安全行为的列表，而是展示了业界确认的、可促进网络安全风险管理的关键网络安全成果。框架核心包括四类要素：功能、类、子类和参考资料，如下图所示：

功能	类	子类	参考资料
识别			
防护			
检测			
响应			
恢复			

框架核心要素如下。

(1) 功能：处于最高级别，包括识别、防护、检测、响应和恢复。组织可利用这些功能管理网络安全风险，包括组织信息、风险管理决策、解决威胁以及通过学习之前的行动进行改善。功能在根据现有方法调整后可用于事件管理，展示网络安全投资的效果。例如，规划与演习方面的投资可促进及时响应与恢复，降低对服务交付的影响。

(2) 类：是功能的下一层级结构，是将功能细分的结果，与计划需求和实际活动密切相关，包括资产管理、访问控制和检测程序等。

(3) 子类：是类的下一层级结构，描述了具体的技术/管理活动结果，子类列举了部分可辅助实现各类目标的结果，包括“外部信息系统编目”、“存储数据保护”和“被调查的检测系统发出的通知”等。

(4) 参考资料：是关键基础设施部门常用的标准、指南和实践，描述了达到子类要求的具

<sup>①</sup> 因篇幅所限，没有对附录进行收录。——译者注

体方法。本框架核心并未列举所有的参考资料，仅列举部分作说明之用。这些参考资料均为框架制定过程中最常引用的跨部门指导手册。

下文解释了框架核心的五个功能，这些功能不是为了形成一个连续的路径，或达到静态的最终理想状态。相反，这些功能可以同时执行，从而形成动态应对网络安全风险的机制。完整的框架核心列表参见附录 A（略）。

（1）识别：促进组织对网络安全风险管理的理解，这些网络安全风险涉及系统、资产、数据以及相应能力。

识别功能是框架有效使用的基础。组织需了解业务环境、关键功能的辅助资源及相关网络安全风险，这样才能根据风险管理策略及业务需求确定事情的优先级。该功能分类包括资产管理、业务环境、治理、风险评估和风险管理策略。

（2）防护：制定和实施相关防护措施，确保关键基础设施服务的交付。

防护功能为限制或遏制潜在网络安全事件的影响提供了支撑。该功能分类包括访问控制、宣传和培训、数据安全、信息保护规程、维护和防护技术。

（3）检测：制定和实施相应防护策略，识别网络安全事件。

检测功能可以及时发现网络安全事件。该功能分类包括异常事件、持续安全监控和检测程序。

（4）响应：制定和实施网络安全事件发生后的优先处理事项和行动。

响应能够为限制或遏制潜在网络安全事件的影响提供支撑。该功能分类包括响应计划、通信、分析、缓解和改进。

（5）恢复：制定和实施相关行动，在网络安全事件发生后，保障功能和服务的恢复能力。

恢复功能将对及时恢复正常运行提供支持，以减少网络安全事件的影响。该功能分类包括恢复计划、改进和通信。

### 框架实施层级

框架实施层级为组织提供了评估网络安全风险的背景以及针对此种风险的现有管理流程。层级包括部分实施、风险告知、可重复和自适应，描述了网络安全风险管理实践中不断增长的严格性和复杂程度以及网络安全风险管理受业务需求影响的程度。风险管理包括网络安全的多个方面，比如在网络安全风险管理和潜在风险响应中，组织对隐私和公民自由的重视程度。

在选择层级时，组织需考虑现有的风险管理实践、威胁环境、法律和监管要求、业务/任务目标和组织机构局限性。各组织应该确定其目标层级，确保所选的层级可满足组织目标，具备可行性，并将关键资产与资源的网络安全风险降低至可接受级别。在确定目标层级时，组织应考虑来自联邦政府部门和机构、信息共享与分析中心、现有成熟模式或其他来源提供的外部指导。

鼓励选择层级 1 的组织向层级 2 或更高层级努力，但层级不代表成熟度。若选择更高层级可降低网络安全风险及成本，则予以鼓励。框架是否成功执行取决于目标轮廓描述的结果是否达成，而非所选层级。各等级层级定义如下。

（1）层级 1：部分实施

①风险管理程序：组织网络风险管理实践为非正式行为，风险管理以临时和反应式的方式进行。网络安全行动的优先级与组织风险目标、威胁或业务/任务需求没有直接联系。

②综合风险管理程序：组织对网络风险知之甚少，且未建立内部网络风险管理措施。网络安全风险管理工作没有正式流程，或仅从外部获得信息。组织内部未形成网络安全信息共享程序。

③外部参与：组织没有形成与其他机构协调或合作的机制。

(2) 层级 2：风险告知

①风险管理程序：组织网络风险管理实践通过了管理层批准，但没有建立组织范围内的风险管理策略。网络安全行动的优先级符合组织风险目标、威胁或业务/任务需求。

②综合风险管理程序：组织意识到了网络安全风险，但未建立适用于组织内部网络安全风险管理措施。组织拥有已批准的网络风险管理流程并获得管理层批准并实施，雇员拥有充分的资源履行网络安全职责，网络安全信息在组织内非正式共享。

③外部参与：组织了解其在更大的生态系统中扮演的角色，但还未形成与外部进行互动和信息共享的能力。

(3) 层级 3：可重复

①风险管理程序：组织网络风险管理实践被正式批准，固化为策略。网络安全行动根据组织业务/任务需求、威胁和技术趋势定期进行更新。

②综合风险管理程序：组织制定了相应的网络风险管理措施，定义了基于风险的策略、流程，并按照计划实施和审查。组织拥有统一有效的方法应对风险变化，人员具备相关知识和技能，可履行既定角色和责任。

③外部参与：组织了解其互依赖关系和合作伙伴，并从这些伙伴处获得信息，以进行协作并在事件发生后做出内部风险管理决策。

(4) 层级 4：自适应

①风险管理程序：组织根据历史经验教训预判未来网络安全变化趋势，调整其网络安全管理策略。通过不断融入先进的网络安全技术和实践，组织可积极应对不断演进、日益复杂的网络安全威胁。

②综合风险管理程序：组织拥有适用于整个组织的网络风险管理方法，这个方法使用基于风险的策略、流程处理潜在的网络安全事件。网络安全风险管理作为组织文化的一部分，由了解历史活动开始，发展到从其他来源获取信息，再持续监控其系统与网络中的活动。

③外部参与：组织与合作伙伴开展积极的信息共享合作，确保所分发及使用的信息准确、实时，以便提高网络安全水平，防止网络安全事件的发生。

### 框架轮廓

框架轮廓将功能、类和子类与组织的业务需求、风险承受力以及资源情况进行匹配。组织可利用轮廓建立一个路线图，以减轻网络安全风险。该路线图需与组织和部门的目标一致，符合法律、监管要求和行业最佳实践，并反映风险管理优先级。鉴于自身复杂性，组织可能会选择多个框架轮廓，以满足组织各部门的个性化需求。

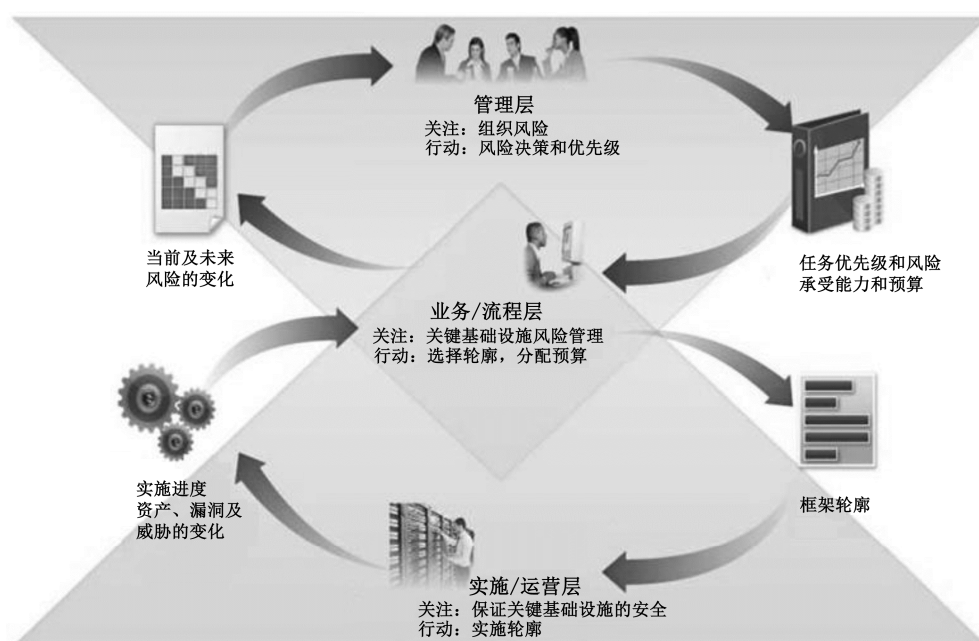
框架轮廓可用于显示网络安全活动的当前状态或期望状态。当前轮廓显示的是目前已经实现的网络安全结果。目标轮廓显示的是期望达到的网络安全风险管理目标。框架轮廓支持业务/任务要求，并协助实现组织内部或组织间进行风险交流。考虑到执行的灵活性，本框架文件不规定轮廓模板。



通过轮廓对比，组织可了解当前网络安全结果与网络安全风险管理目标之间的差距。制定能够消除这些差距的行动计划，有助于实现上述路线图。可根据组织的业务需求和风险管理流程，确定缩小差距的优先级。采用基于风险的方法，组织可衡量资源评估情况，并按照优先级，以经济有效的方式实现网络安全目标。

### 协调框架实施

下图描述了信息和决策在某个组织的管理层、业务/流程层、实现/运营层的流动情况：



管理层就任务优先级、可用资源和总体风险承受力与业务/流程层进行沟通。业务/流程层将沟通结果作为风险管理流程的输入，与实现/运营层沟通业务需求并建立轮廓。然后实现/运营层就轮廓实现进度与业务/流程层进行沟通。业务/流程层基于这些信息进行影响评估，然后将影响评估结果上报管理层，从而将组织内的整体风险管理流程传达给实现/运营层，让其了解风险对业务的影响。

## 3. 如何使用本框架

各组织可将本框架作为识别、评估和管理网络安全风险这一系统流程的关键部分。本框架并非要取代现有流程。组织仍可使用当前流程，将其与框架相叠加，以确定当前网络安全风险方案与风险管理目标之前的差距，并制定路线图来缩小差距。组织可将本框架作为网络安全风险管理工具，以确定对关键服务交付而言最重要的活动，并对开支进行优先级排序，确保投资影响最大化。

本框架是对现有业务和网络安全运营的补充。组织可根据本框架构建新的网络安全计划或建立当前计划提升机制。框架提供了一个向业务伙伴和客户表达网络安全需求的手段，并协助组织明确网络安全实践与安全目标之间的差距。同时，本框架提供了网络安全工作可能涉及的

隐私和公民自由等注意事项和流程。以下列举了几种对框架的使用方法。

### 对网络安全实践进行基础性评估

本框架可用于将组织当前的网络安全活动与框架核心内容进行对比。通过建立当前轮廓，组织可确定其对于核心类和子类中结果的实现程度。这些结果对应于框架的 5 个高级功能：识别、防护、检测、响应和恢复。有的组织可能会发现其既定目标已实现，因此网络安全管理只针对已知风险。而有的组织可能认为还有提升空间。这些组织可利用此类信息实施行动计划，加强现有的网络安全实践，降低网络安全风险。还有的组织可能认为针对某些目标投资过度。这些组织可基于此类信息重新确定资源优先级，以加强其他网络安全实践。

尽管这些组织仍采用原有的风险管理流程，但本框架的 5 个高级功能使管理人员和其他人员很容易地提取网络安全风险的基本概念，这样他们就能够评估组织是如何管理已识别的风险的。此外，本框架能帮助组织了解当前工作进展。必要时，组织可在充分知情的情况下提升其网络安全实践。

### 制定或改进网络安全计划

以下步骤阐述了一个组织如何利用本框架建立新的网络安全计划或改进现有计划。为实现网络安全状况的持续提升，可根据需要重复采取以下步骤。

(1) 步骤 1：确定优先级和范围。组织确定其业务/任务目标和整体优先级，制定与网络安全实施相关的战略决策，并确定支撑业务或流程的系统和资产的范围。本框架需支持组织内的各业务线或流程。这些业务线或流程可能会有不同的业务需求和风险承受能力。

(2) 步骤 2：确定方向。组织在明确了需纳入网络安全计划的业务线和流程之后，需确定相关系统和资产以及监管要求和整体风险管理方案。此外，组织还需识别这些系统和资产面临的威胁及存在的脆弱性。

(3) 步骤 3：建立当前轮廓。组织可建立当前轮廓来展现框架核心中的类和子类的执行结果。

(4) 步骤 4：评估风险。组织可依据总体风险管理流程或之前的风险管理活动进行风险评估。在评估时，组织需分析运营环境，判断是否有网络安全事件发生，并评估事件对组织的影响。重要的是组织需根据新的风险、威胁和脆弱性信息，来识别网络安全事件及其影响。

(5) 步骤 5：建立目标轮廓。组织创建一个目标轮廓，用于评估其期望的网络安全结果的框架的类和子类。同时，组织还可以制定自己的类和子类，以解决其特有的组织风险。此外，组织还需考虑外部利益相关方的影响和需求。

(6) 步骤 6：确定、分析和缩减差距。组织对当前轮廓和目标轮廓的分析结果进行比较，找出差距，然后制定一份优先执行的行动计划来消除这些差距。该计划基于组织业务驱动、成本/收益分析和对风险的理解，从而实现目标轮廓中规划的目标。之后，组织确定消除这些差距所需的资源。通过利用这些轮廓，组织可针对网络安全活动做出明智的抉择，进行风险管理。

(7) 步骤 7：实施行动计划。组织决定针对这些差距采取哪些行动，然后根据目标轮廓监控当前网络安全实践。为提供进一步指导，本框架还确定了有关类和子类的参考资料，而组织应确定哪些标准、指南、实践，包括各行业特有的标准、指南和实践，能够最有效地满足自身的需求。

组织可能会根据需求重复执行以上步骤，持续评估和提升其网络安全。例如，组织可能会发现多次执行步骤 2 可提升风险评估质量。此外，组织可通过当前轮廓的迭代更新监控风险评

估进度，随后将当前轮廓与目标轮廓提供的结果进行比较。利用该流程，组织的网络安全计划将更加贴近框架实施层级。

### 与利益相关方沟通网络安全需求

本框架提供了通用语言，方便组织与负责关键基础设施服务交付的相关利益相关方进行需求沟通。例如：

- 组织可通过目标轮廓向外部服务提供商提出网络安全风险管理需求。
- 组织可通过当前轮廓传达其网络安全状态，上报结果数据或将其与采购需求进行比较。
- 关键基础设施的所有者或运营者在确定了基础设施所依赖的某个外部利益相关方后，可使用目标轮廓传达所需的类和子类。
- 关键基础设施部门可建立一个目标轮廓，作为初始基线轮廓供员工使用，并在此基础上逐步定制自身目标轮廓。

### 为确定新参考资料或修订参考资料提供机会

本框架可用于确定新的或修订的标准、指南或实践，新增的参考资料将有助于满足组织新需求。组织在实现特定子类或开发新子类时，可能会发现手头仅有少量参考资料。为解决此问题，组织可与技术领导者和（或）标准制定机构合作起草、研制或协调标准、指南或实践。

### 保护隐私和公民自由的方法

本节介绍了行政令所要求的一种用于解决网络安全操作可能导致的个人隐私和公民自由问题的方法。鉴于个人隐私和公民自由因部门和时间的推移而异，该方法应包含一套通用的注意事项和流程。组织可通过一系列的技术实现来满足这些注意事项和流程要求。然而，并非安全计划中所涉及的所有活动都需要考虑这些注意事项。组织应参考上一节制定技术涉及的隐私标准、指南和实践，为技术实现改进提供支撑。

当组织的网络安全活动需使用、收集、处理、维护和披露个人信息时，可能会引起隐私和公民自由问题。以下活动可能会涉及隐私或公民自由问题：网络安全活动中对个人信息过度收集或存储；使用或披露与网络安全活动无关的个人信息；风险减缓活动可能造成拒绝服务或其他类似的潜在不利影响，包括可能影响言论或结社自由的事件检测或监控。

政府及其代理机构对网络安全活动导致的公民自由问题负有直接责任。例如，政府或拥有、运营关键基础设施的政府代理机构应出台合理的流程，使其网络活动符合现有的隐私法律、法规和宪法要求。

为解决隐私问题，各组织应考虑如何使其网络安全计划遵循隐私原则。例如，网络安全活动涉及个人信息收集、披露和保留时，应确保数据最小化；对超出网络安全活动范围之外搜集信息的行为进行限制；增加某些网络安全活动的透明度；网络安全活动中使用个人信息前需得到个人同意，一旦造成负面影响，应进行相应赔偿；数据质量、完整性和安全性以及问责和审计。

在附录 A 的“框架核心”中，以下流程和行动可被视为解决上述隐私和公民自由的方法：

#### （1）网络安全风险治理

- 组织对网络安全风险和潜在风险响应的评估要考虑到网络安全工作中涉及的隐私问题。

- 负责网络安全隐私保护的员工要训练有素，能够及时发现有关问题并上报管理人员。
- 制定相关流程，确保网络安全活动符合适用的隐私法律、法规和宪法要求。
- 制定相关流程，对上述组织措施和控制措施进行评估。
- (2) 对访问组织财产和系统的人进行标识和鉴别的方法
  - 采取措施来标识和解决访问控制措施所导致的隐私问题。这些访问控制措施涉及个人信息的采集、披露或使用。
- (3) 安全意识和培训措施
  - 将组织隐私策略中的有关信息纳入网络安全人员培训和安全意识提升活动之中。
  - 将组织的隐私策略传达给为其提供网络安全服务的供应商。
- (4) 异常行为检测以及系统和资产监控
  - 制定相关流程，对组织的异常行为检测和网络安全监控活动进行隐私审查。
- (5) 响应活动（如信息共享或其他缓解措施）
  - 制定有关流程，评估并考虑以下问题：个人信息是否作为网络安全信息共享活动的一部分在组织外进行共享？何时共享、如何共享以及共享程度？
  - 制定有感流程，对组织的网络安全风险缓解措施进行隐私审查。

---

## 二十六、网络威慑政策报告

美国白宫

2015 年 2 月

---

## 1. 前言

在过去的 30 年中，美国越来越依赖于网络空间，作为促进全球商品和服务流动、促进自由和开放的政治对话，以及支持大量诸如电力控制、水和其他公共事业类关键服务的方式。虽然互联网带来了无与伦比的社会和经济机遇，但也为国家和经济安全，敏感企业和个人信息安全带来了艰难挑战。在一个全球连接的世界之中，对 21 世纪美国及其盟友而言，网络安全是最严重的国家安全方面的担忧。

社交、移动和互联网技术的发展在全球范围内一直伴随着网络相关风险的扩散。精明且有技术能力的人员会实施欺诈、盗窃、破坏、操纵行为，并且在某些情况下会破坏计算机系统、网络或数据。罪犯、恐怖分子和民族国家的敌人能够趁美国在普遍使用但却显脆弱性的技术去篡改、窃取或破坏信息，转移或偷盗金钱，窃取知识产权来获得竞争优势，并且有可能破坏关键基础设施。

网络空间中的绝大多数风险不会对个人或公共安全，甚至国家的运行、经济或社会造成严重的威胁<sup>①</sup>。与此同时，网络攻击和某些恶意网络活动<sup>②</sup>，尤其是民族国家或具有强大能力的非国家行为体实施的攻击，以及以美国境内关键基础设施和重点产业为目标的攻击，会对美国的国家安全和经济利益构成严重威胁。正是这些重大威胁，使美国政府力求通过在网络空间威慑敌人的政策来应对<sup>③</sup>。美国政府正在采取多方面的政策努力，以期利用所有的国家力量工具来应对对国家有重大威胁的恶意网络活动，并阻止民族国家或非国家行为体利用网络手段对美国造成伤害。我们不会破坏互联网的开放和互联质量，正是这才使互联网成为一个全球经济和社会进步的强大推动力。在这个过程中，政府将会不断完善目前的能力并开拓创新，面对美国及其利益方遇到的恶意网络活动，提高攻击的成本，或降低攻击的收益。

## 2. 美国将试图威慑什么

美国政府的政策是利用所有的国家力量工具来威慑对美国及其重大利益构成严重威胁的网络攻击和其他恶意网络活动。具体而言，这包括破坏关键基础设施和重要服务，由此对生命造成威胁；破坏对关键功能支撑系统的信心和信任度，包括军事指挥和控制、金融市场的有序运行；对隐私、言论自由等核心价值造成危害的国家级威胁。以下列举了威慑活动所关注的优

---

① 所有的恶意网络行为都受到美国政府的关注，且很多保护美国公共-私营网络、保护公民和商业、向行为者追责的活动、项目和其他努力都针对这些恶意行为。

② 本文中，**网络攻击**指对计算机、信息或通信系统、网络、计算机控制的物理或虚拟系统实施拒绝访问、中断、报废、降级、破坏或停运等手段。网络攻击有很多直接或间接的影响，程度各不相同。美国的威慑主要侧重于那些会导致死亡、关键基础设施受损、巨大财产损失，或使美国及其利益方的国家安全、外交政策、经济繁荣或金融稳定受到严重威胁的攻击。**恶意网络活动**指试图破坏计算机、信息或通信系统、网络、计算机控制的物理或虚拟系统及其存储或传输的信息的保密性、完整性或可用性的活动。

③ 虽然美国政府的网络威慑工作主要侧重于美国利益受到的重大威胁，但本报告中列出的框架，包括“整个政府层面”的方法，也可用于威慑比其级别低的威胁，这一般通过非军事手段实现。

先领域。不过，其既不是全面的，也不会一成不变，我们将根据新威胁和地缘政治的发展调整优先事项。特别是，政府最关心的是有可能对美国及其利益方造成大规模破坏、毁灭、生命损失和重大经济后果的威胁，包括但不限于：

- 旨在造成人员伤亡的网络攻击和其他恶意网络活动。
- 旨在对美国社会或政府的正常运转造成严重干扰的网络攻击和其他恶意网络活动，包括对关键基础设施的攻击，这将破坏向公众和政府提供关键服务<sup>①</sup>的系统。
- 威胁到美军的指挥和控制、美国军事力量的自由调遣，或美国军方赖以维护美国利益和承诺的基础设施的网络攻击和其他恶意网络活动。
- 通过网络经济间谍或破坏来危害国家经济安全的恶意网络活动。此类活动破坏了全球经济的公平性和透明度，如美国的竞争对手窃取那些正在开发中的技术、通过不公平手段赢得合约，或窃取信息来操纵市场以直接利益其公司。

恶意行为者会采用各种策略来攻击、利用或扰乱网络、系统及数据。敌人正在试图潜入高强度防护、隔离或强化的网络，如那些被很多美国实体用于履行重要的国家安全和经济职能的网络，它们可能会结合技术和精巧的人力手段。尽管干这类事情要具备全面的攻击能力，包括资源、毅力和技术专长，但是没有哪个方法是民族国家所独有的。主要的攻击方法包括以下几种。

- 远程网络攻击：通过网络空间侵入目标机器、网络和信息。这些活动会利用网络和个人计算机的技术漏洞、不正确的配置以及人为错误。很多远程攻击也依靠不知情的受害者接收了某种消息或文件，而其中嵌入了可损害其系统的恶意软件（恶件）。
- 供应链攻击：侵入提供给预期受害人的产品和服务。这些活动可能会发生在产品生命周期的任何时间点，包括设计、制造、分发、维护或升级，并能把从微元器件到整个系统的一切事物作为攻击目标。
- 邻近访问攻击：企图拦截不受保护的无线通信和目标系统附近泄露的其他电磁信号，包括被入侵的硬件或主机发出的隐性信号。
- 内部威胁：有意或无意地提供关于目标网络的信息，从其他人处搞到信息，破坏系统或数据，或影响目标组织的决策。蓄意的内部攻击会窃取便携的媒体信息和文件，或者安装设备或软件，以有利于其采集和窃取信息。

### 3. 网络威慑战略

威慑是要说服敌人，即影响他们的决策制定，不要有威胁到重要国家利益的行为。施加影响的手段是，令人毫不质疑地展示其使敌人无法获利和提高敌人成本的能力及意愿，以去说服敌人“比起对抗，约束自己会有更好的结果”。但信息时代的网络威慑与冷战时期的威慑概念有本质上的不同。冷战时期的威慑概念旨在慑止大规模杀伤性武器的使用，少数拥有核武器的国家与美国或苏联结盟，形成两极国际体系。如今，美国拥有占优势的军事能力，但却不对称地依赖于网络空间，并面临着能力强的国家和非国家潜在敌人，他们具备对美国发动重大网络

① 第 21 号总统政策令（PDD21）《关键基础设施安全和恢复力》确定了 16 类关键基础设施，它们对美国政府异常重要，包括：化学，商业设施，通信，关键制造业，大坝，国防工业基地，应急服务，能源，金融服务，食品和农业，政府设施，健康和公共服务，信息技术，核反应堆，核材料和废弃物，运输系统，水和废水处理系统。

攻击的能力、技能和意向。此外，很多网络工具是两用或多用途的，可实施一系列恶意网络活动。比起传统军事能力，网络工具和活动可使用较少资源来研发，以相对较低的风险实现广泛的作战范围，并能以合理的方式予以否认，这些特征同步催生了对这种能力的渴求并降低了能力建设的门槛。

网络空间还具有其他鲜明特征，包括全球性、互联性、主要由私人拥有、匿名性和破坏者的低进入壁垒。同很多传统领域的威慑比起来，网络空间威慑在种类和范围方面有很多不同，这为其增加了挑战。更复杂的问题是，潜在敌人可能没有相等的网络能力，并且双方都不太可能知道另一方的能力水平。虽然通过长期分析，美国对网络攻击的归因能力在近年来已经有了显著提高，但是对于追究恶意网络活动行为者的责任，高可靠性的实时归因<sup>①</sup>分析仍然很困难。最后，恶意网络工具可用于实现多重目的，从骚扰到破坏，并且不会造成大规模杀伤性武器那样的破坏性影响。考虑到网络威胁的这些特征，美国政府将采取多元方法来制定网络威慑战略与战术。

#### 4. 美国网络威慑政策的组成要素

鉴于网络空间的特点，美国在反恐主义和防扩散领域的经验是与此高度相关的。政府从中认识到，使用广泛的威慑概念是应对能力与信息均呈不对称态势的一种重要手段。这种威慑概念使用“全政府”方法调动国家权力的所有元素，向特定的威胁施加压力。网络威慑政策依靠所有的国家力量作为工具：外交、信息、军事、经济、情报和执法以及公共-私营合作关系，目的是使敌人在心理上对所有恶意网络活动效果产生不确定性，并增加敌人因自身行为需要付出的成本和承担的后果。

- 拒止威慑：使敌人相信美国能遏止恶意网络活动，从而减少敌人实施这些活动的动机。为此，美国必须部署强大的防御系统并构建体系结构上具备韧性的系统，以便在遭受攻击或其他破坏事件后迅速恢复。
- 通过成本强加来实现威慑：这些措施旨在使那些对美国进行网络攻击或其他恶意网络攻击的敌人面临惩罚和高昂成本。这些措施利用美国政府在能力和意愿方面的优势，通过所有必要的手段来应对网络攻击，并确保方法适当、与国际法保持一致。这些措施包括但不限于付诸执法手段、制裁恶意网络行为者、进行攻击性和防御性网络操作以及通过陆、海、空、天来投射力量，并在用尽所有可用选项后使用军事力量。

##### 拒止威慑

- 实施防御、韧性和重建行动，为关键网络提供更强大的能力，以防止或减轻网络攻击或其他恶意网络活动的影响，并在受到攻击后快速重建系统。
- 构建与私营部门之间的稳固合作关系，以促进网络安全最佳实践；使公众建立对网络安全措施的信心；提高国家在增强网络韧性工作方面的公信力。

虽然以实时方式实现（归因的）高可确定性是困难的，美国还是不断提升对恶意网络活动的归因能力，就是要使恶意行为者对其所作所为负责。美国成功威慑国家和非国家发起的网络

---

① 本文中，“归因”定义为判断直接网络攻击者或其他恶意网络行为责任人的身份和位置的能力。



威胁的能力至少要依靠防御战略，以增高技术或其他类型的壁垒，这同传递美国能够也必将妥善应对网络威胁这一信息一样重要。要确凿无疑地实现这一事实：即使是面对复杂的网络威胁，美国也能保持强健的防御能力，确保拥有韧性的网络 and 系统，实现强大的可以投射力量、保护美国利益的反应能力。

美国政府认识到，一些网络和基础设施以及它们支持的任务比其他的更重要，应得到相应的保护。因此，政府的网络威慑政策旨在展现政府和私营部门的网络防御力量，使攻击者去怀疑自己的攻击能否成功或能否达到预期效果。这种改变敌人风险-收益算式的做法可以使得敌人无所事事，并且不需要进行归因。

为了加强网络防御，美国政府要同私营企业合作，确定必须得到保护的关键系统，并实施网络安全的最佳实践。同时，政府也改进了政府部门之间、政府与私营部门之间的网络威胁指标的信息共享。此外，美国政府还在改善自身信息安全、确保重要计算机系统和网络韧性方面做了大量投入，包括发展快速重建能力、降级操作能力以及在必要时宕机也能维持业务功能的能力。

#### （1）确定并保护关键基础设施

要全天候保护所有系统、防范任何一种网络攻击，这种想法是不切实际的。无处不在的软件 Bug 和其他漏洞意味着美国政府不能保证所有系统永远免于入侵或破坏。比起在所有时期试图保护所有系统，美国政府会将其工作优先级放到确定并防护关键基础设施上面。政府的努力和资源将优先投入于这些特定系统，确保其受益于不断改进与发展的网络安全和网络防御措施。

为了解决这个问题，美国国土安全部（DHS）在 2013 年被赋予了实施第 13636 号行政令第 9 节的任务，其中规定：

“本令发布后 150 天内，国土安全部长将使用一种基于风险的方法来确认关键基础设施，即这些关键基础设施发生的网络安全事件能对公共健康或公共安全、经济安全或国家安全造成毁灭性的地区或国家级影响。”

为了开展这项工作，国土安全部咨询了代表所有 16 个关键基础设施部门的系统所有者及运营者，以及关键基础设施的对口部委、部门协调委员会、政府协调委员会、独立的监管机构和专家。通过这种合作和研究，已在几个关键基础设施领域确定了一些小的子集实体。这些实体发生的网络安全事件和其二阶、三阶效应可能会导致在公共健康或公共安全、经济安全和国家安全等方面造成毁灭性的地区或国家级影响。国土安全部将继续每年都与合适的利益相关方审查和更新这个列表。

基于这些结果，国土安全部和美国政府的其他部门已经建立了基础条件和流程制度，以向标识出的关键基础设施所有者和运营者传播具体、有针对性的网络安全威胁信息。这些信息可被用于检测和阻止有入侵企图各类网络敌人。国土安全部正在与更广泛的关键基础设施所有者和运营者合作，以理解其网络和系统受到的网络攻击可能产生的级联效应。这些工作正在提高私营部门检测和阻止入侵企图以及从各类网络事件中恢复的能力。这种公共-私营合作也塑造了政府面对重大网络安全事件的规划、减轻损失和响应工作。

#### （2）分享威胁信息

共享网络安全的态势感知和网络恶意活动的迹象信息，包括共享攻击行为者的信息，为网络防御者们提供了在已知漏洞被全面利用前将其关闭的机会。因此，美国政府正在政府和私营部门之间扩大其现有的信息共享机制。很多工作是通过将现有项目进行扩张而完成的，包括国

防工业基地网络安全和信息安全保障计划，国土安全部的增强网络安全服务项目，受保护的关键基础设施信息项目，以及在私营部门参与下的一些项目。但是，也还有很多工作需要继续做。

第一步，政府正在努力降低现有规制下合理实现信息共享所面临的可能及现实的障碍。例如，美国司法部（DOJ）和联邦贸易委员会在 2014 年 4 月发布的指南已经指出，反垄断法不会对企业之间开展合理的网络安全信息共享构成障碍。但要改进美国网络安全，长期看需要进行立法，允许工业界能够便捷地在全国范围以协调的方式同政府共享网络安全信息。政府将同国会在立法上继续努力，厘清可以共享的网络安全威胁和信息类型，尤其是来自私营部门向政府共享的信息，并共同开发或支持建设有利于信息共享的机制。具体而言，政府将继续推行立法，鼓励私营部门与国土安全部的国家网络安全和通信整合中心（NCCIC）共享网络威胁信息。国家网络安全和通信整合中心（NCCIC）负责向相关联邦机构，以及私营部门建设与运行的信息共享和分析机构（ISAO）共享准实时信息。为鼓励私营部门的信息共享，目前政府在立法建议中，对公司同 NCCIC 及 ISAO 之间开展信息共享提供了针对性的责任保护机制。

政府在网络安全信息共享上的所有工作也将努力确保隐私和公民自由得到了保护，并指明了民事和情报机构各自的角色和任务。根据政府目前的立法建议，与联邦政府分享信息的私人实体必须遵守某些隐私限制，如删除不必要的个人信息并采取措施保护必须共享的个人信息，以获得责任保护资质。该提议进一步要求，国土安全部和总检察长要咨询隐私和公民自由监督委员会及其他单位，为联邦政府制定接收、留存、使用和披露信息的指引。

### （3）通过“网络安全框架”促进最佳实践

2013 年 2 月，奥巴马总统签署了增强关键基础设施网络安全的第 13636 号行政令。其中，要求美国国家标准与技术研究院（NIST）主导制定一种网络安全最佳实践模板。2014 年 2 月，NIS 发布了模板的第一个版本“网络安全框架”。其参考了全球公认的标准和实践，以帮助一个组织了解、沟通和管理其网络风险。

美国的企业已经开始在很多经济部门采用并实施该框架<sup>①</sup>。这意味着很多组织正在提高其整体网络安全基线，通过实施基于标准的措施来保护其最敏感的信息，关闭网络中的已知漏洞，为实现基本的网络安全防御而对软硬件进行投入。政府将继续推动对该框架的采用，以将其作为改善美国网络防御的主要手段，同时降低敌人通过从事恶意网络活动而获利的预期。

### （4）抵御内部威胁

在一连贯的未授权泄露涉密信息的事件中，包括“维基揭秘”事件和美国情报计划的泄露，都来自于敏感计算机网络的内部破坏，美国政府已加大了对加强涉密信息保护、降低内部人员威胁等方面的政策与行动的关注。2011 年 10 月，奥巴马总统发布了第 13587 号行政令，要求进行结构化改革，以确保对涉密信息的负责任共享和防护，并建立了高级信息共享和防护指导委员会、信息防护执行局以及国家内部威胁工作组（NITTF）。

- 高级信息共享和防护指导委员会：由管理和预算办公室高级代表和国家安全委员会工作团队共同主持，确保在各部、局间建立高级责任制，以监督各部、局实施计算机网络涉密信息共享和安全防护政策与标准的情况。
- 信息防护执行局：在国防部长和国家安全局局长的共同领导下，制定有效的技术防护

---

<sup>①</sup> 例如，2015 年 2 月 13 日，在白宫的网络安全和消费者保护峰会上，英特尔、苹果、美洲银行、美国银行、太平洋瓦斯和电力公司、美国国际集团、QVC、沃尔格林、凯撒医疗均宣布，承诺采用“网络安全框架”。

政策和标准，以解决这些系统中的国家安全系统和涉密信息的安全防护问题。

- 国家内部威胁工作组：在司法部长和情报局长的共同领导下，汇集了政府各部门的安全、反情报和信息保障专家，建立一个政府范围的内部威胁项目，以阻止、检测和减轻内部威胁，包括涉密情报的泄露。

#### （5）强化政府的网络防御能力

联邦政府不断通过广泛实施的网络安全功能和服务来提高其信息和系统的安全性，以检测和防止恶意网络活动，以及更有效和更安全地管理内部网络与系统。虽然这些工作正在迅速扩张，但是美国政府的系统和网络仍是易受攻击的。为了应对这一挑战，政府正在要求各部、局负起责任，通过“网络安全跨部门优先目标”<sup>①</sup>来提高其网络防御水平。在此情况下，美国政府正在为各部、局设置明确的网络安全目标，并对其完成目标的结果进行追责。同时，政府正在改进对网络安全资金投入进行跟踪的能力，以强化资源与结果的关联度。

除保护联邦网络外，国防部（DoD）正在持续提高军事和国防工业企业的网络防御水平，以保护无数网络设备和数以千计的储存涉密和非涉密军事信息的飞地。美国网络司令部与各现役网络战分队、国家安全局和国防信息系统局一起，监测着国防部网络的运行，并定期向这些网络的运营者提供威胁和漏洞信息。国防部还致力于通过建立联合信息环境（JIE）来完成整体架构和网络防御体系的现代化，这将基于共享的基础设施、企业级服务和一致的安全体系结构，实现安全的互联网通信和情报服务。

除了防御措施，美国政府也必须确保其网络、系统和数据的灵活性。为此，政府已实施的政策是要提高联邦政府发现和应对突发事件的能力，以及在攻击后迅速重建的能力。在 2013 年，政府发布了关于关键基础设施的安全性和恢复力的第 21 号总统政策令（PPD-21），其重点是推动国家团结努力，去强化和维护关键基础设施的安全、功能与韧性。第 13636 号行政令（E.O.13636）与 PPD-21 同时发布，还要求努力保护关键基础设施。E.O.13636 规定了联邦机构要同私营部门共享网络威胁信息，并开发网络安全框架，目前很多联邦机构正准备采纳。这些改善政府网络安全信息共享和风险管理的工作，不但可以加强态势感知、事件检测和预警能力，反过来也可以帮助政府部门的网络防御人员做好应对攻击的准备和提高政府系统的快速恢复能力。最后，联邦各部、局还将网络安全作为其持续运营计划的一个越来越重要的组成部分。

#### 通过成本强加方式实现威慑

- 提出可以用来提高恶意网络活动行为者的**经济成本**的多种选项。
- 寻求适当的**执法行动**，从而（1）对从私营部门或政府窃取信息，以及危害、扰乱、破坏美国计算机和网络的网络罪犯，进行调查和起诉；（2）阻止敌人接触用以实施恶意网络活动的基础设施。
- 必要时，提出适当的军事选项，**保卫国家免遭网络攻击**。

与联邦政府在 2011 年发布的《网络空间国际战略》一致，并依据国际法赋予的权利，美国政府保留使用所有必要手段——外交、信息、军事及经济手段的权利，来保护国家和美国利

① “跨部门优先目标”框架根据 2010 年《GPRA 现代化法》建立，用于加速推进为数很少几个由总统确定的优先领域的项目，这些优先项目的实施往往需要多个政府部、局的合作与协调。在总统行政办公室和主要部、局内，每个目标都有一个指定的高级官员。关于该框架的其他信息可见 <http://www.performance.gov/cap-goals-list/>。

益，防止受到恶意网络活动的危害。在网络空间发生的攻击并不意味着必须通过网络手段进行合法和适当的反应，也不意味着直接反应是最合适和最相称的。相反，美国必须保持多种反应能力，便于为总统和美国其他高级领导人提供选项，根据特定的敌人、恶意活动影响以及归因的把握性等，对选项进行裁剪。

#### （1）提高恶意网络行为者经济成本的措施

经济工具可以提高恶意网络行为者的成本，阻止某些网络威胁，特别是针对那些以非法获取商业秘密来危害美国经济安全，包括知识产权或受控技术的敌人。在适当并经批准的情况下，政府将会采取行动，增大恶意网络行为者的经济成本，包括当这些活动违反了国际贸易规则或世界贸易组织（WTO）规则时。

特别地，金融制裁可以为应对网络攻击提供一种有效的工具。为了应对朝鲜在 2014 年 11 月发起的破坏性、高强度的网络攻击（这次攻击旨在损害美国的商业并压制言论自由），美国政府宣布对已查明的朝鲜攻击者实施新一轮制裁。此外，2015 年 4 月，总统发布了一个新的行政令，授权向对国家安全、外交政策、经济繁荣或金融稳定造成重大威胁的个人和实体实施制裁。制定这项政策时，政府是在创建一种提升对方成本的方式，不仅针对网络攻击者，也针对那些支持、启动或命令那些攻击的人或组织。美国政府已经使用这些工具来应对其他方面的政策挑战很多年了，并会继续将其用在防止和应对网络威胁方面。

#### （2）采取执法行动

执法也可以是对网络威胁的一种有效威慑，不论是用在拒止威胁方面（如阻断某个用来实施攻击的僵尸网络），还是成本强加方面（如将网络攻击者绳之以法）。虽然调查和起诉在网络环境下是具有挑战性的，但美国政府还是可以使用该工具有效地破坏和降低敌人的网络能力。执法界通常使用传统的调查技术、取证工具、秘密行动、保密的人力资源以及合法授权的监控来调查未经授权入侵和攻击计算机与网络的事件，所有这些方法都能帮助发现个体和组织构成的网络威胁。

##### ①调查、检控并中止恶意网络活动

由于每次入侵的背后都有一个个体或组织，美国执法机构构成了美国政府网络事件响应机制的关键因素。它们定期公开调查针对美国受害者的恶意网络活动，并且当有证据支持时，司法部会根据《联邦起诉原则》起诉那些行为人。成功的调查和起诉会给恶意网络行动者以及支持或庇护他们的国家强加直接成本，这会有助于阻止这些人或组织继续实施此类活动。

执法还可以使敌人无法访问那些用以对美国进行恶意网络活动的基础设施。例如，如果某个敌人开发和使用了一个僵尸网络，威胁到或实际上破坏了某类重要的公共服务，执法机构可能不仅要调查和起诉涉嫌肇事者，还要打击僵尸网络本身。利用执法的能力和权力，美国政府可以不断调查和打击恶意网络活动，并起诉那些危害美国的犯罪分子。这种成功的执法工作可以威慑那些试图使用网络手段来危害生命安全、破坏社会、政府或重要公共服务运行的铤而走险者。

##### ②建立打击网络犯罪的国际合作能力

打击网络犯罪不仅是一个国内问题。很多敌人使用外国的基础设施来实施入侵或破坏活动。协助其他国家建设调查、起诉并打击网络犯罪活动的符合美国的利益。通过美国主导的课程，美国正在帮助其他国家发展这些能力，主题多种多样，从网络相关的法律框架、使用取证工具到调查犯罪。此外，美国政府还鼓励其他国家加入《布达佩斯网络犯罪公约》以及

使用公约的结构作为能力建设的基础。该框架包括三个关键概念：（1）确保执法机构有权限和工具来调查网络犯罪和处理电子证据；（2）制定实体性的网络犯罪法律；（3）使用诸如 24/7 的打击高科技犯罪网络机制来确保有效和及时的国际合作。美国政府正重新推动增加“布达佩斯公约”缔约方的数目，并增加 24/7 网络的会员资格，以便于建设执法联络点。已有 53 个国家加入了“布达佩斯公约”，其中有 44 个国家批准其进入了本国法律。总体而言，政府在推动建设国际合作关系方面正在取得进展，无论在哪里都必须将犯罪分子绳之以法，这样便可以对那些严重威胁我们国家安全和经济利益的人形成另一种威慑。

### （3）在网络空间建立保卫国家的能力

美国政府的第一选择是使用网络防御、执法措施、经济行动和外交来对抗、阻止并缓解网络事件。然而，当防御和威慑力度不够的时候，美国政府必须拥有保护国家网络空间的能力。在总统的指挥下，美国政府将做好使用所有必要手段的准备，包括军事手段，以应对国家受到的网络攻击。

为了支持这一要求，国防部在 2010 年 10 月建立了美国网络司令部，以巩固美国军事网络应对网络威胁的能力。在与其他作战司令部的协同下，美国网络司令部正在建造一支高水平的队伍。网络任务部队能够实施全面的网络操作，并为保卫国家做着持续规划和准备。2013 年 9 月，美国网络司令部激活了其“网络国家任务部队”的总部，这是其三个不同任务部队之一<sup>①</sup>，可以迅速对美国受到的网络攻击做出反应。通过采取这些措施，国防部为总统建立了可靠和可信的选项，以威慑那些试图在网络空间发起攻击的敌人，并捍卫国家免受网络攻击。

此外，如果得到指令，国防部可以实施网络空间作战任务，包括攻击性网络作战。第 20 号总统政策令制定了政策框架，以便管理这种网络作战行动。虽然美国政府不是只能在网络空间对网络攻击进行响应，但这种对称性反应确有独特优势。网络作战可以精确裁剪到只指向对美国进行攻击的系统。此外，打击恶意系统的方法可以是足够精确的，以尽最大可能减少附属影响。发展这些能力并不意味着美国对网络空间的军事化超过对海洋的军事化。然而，试图探测美国决心的敌人应该明白，在网络防御和执法措施不足的情况下，美国是可以使用网络作战来保护我们的国家和利益的。

### 支持网络威慑的活动

- 采取“整个政府层面”和“整个国家层面”的方法，对网络事件做出响应，并应对国家级事件。
- 一点一滴地、累进不断地推进**政策声明**和**战略通报**，强调美国政府对动用其能力抵御网络攻击的承诺。但在针对网络威胁采取回应和使敌人承担后果方面，仍然保持一个不明确的底线，以防止敌人在底线以下进行恶意网络活动。
- 进一步发展**情报能力**，即提升美国对于恶意网络活动的归因分析和行动能力，以理解敌人的计划和意图，确定敌人认为有价值的美国目标，并挫败敌人的活动。
- 增强**国际接触**，以建立网络空间国家行为规范，提高集体网络防御能力，促进打击网络犯罪方面的合作，强化结盟，对关键基础设施受到网络攻击时应采取何种适当响应达成共识。

---

<sup>①</sup> 另外两支部队是：网络战斗任务部队，支持司令部的作战需要；网络保护任务部队，保护国防信息网（DoDIN）。

- 开展**研究与开发**，以降低并最终消除敌人的不对称优势，发展可监控并检测敌人活动的新能力，在网络空间追踪敌人，并以可衡量的方式挫败敌人。

(1) 增强“整个政府层面”和“整个国家层面”的反应能力

随着网络事件的速度和规模呈指数级增长，美国政府认识到，网络风险可以被显著降低，却不可能根除。此外，没有一个政府部门有必备的能力或权限单独处理威胁。每个联邦部、局都要拥有特别的专业知识来应对这个问题。国务院则利用其与外国政府的关系来协调政策响应。司法部和联邦调查局（FBI）具有相当大的调查、起诉以及执法的能力和权力。美国国土安全部充分掌握了美国关键基础设施的相关信息，以及拥有在事件响应、风险缓解方面的大量技能，并与私营部门保持着深厚关系，这对保护关键基础设施和应对网络攻击是十分必要的。美国特勤处拥有对大规模网络欺诈调查的技能，这有可能产生国家级影响。移民和海关执法、国土安全局负责调查与在线盗窃知识产权、出口受控数据有关的网络犯罪以及很多其他通过网络实施的犯罪，包括儿童剥削、网络走私和地下黑市。经济部门，包括商务部、财政部、美国贸易代表办公室可以利用其对经济和市场的力量以及各自的授权来实施经济制裁、执行贸易法，以及采取其他针对恶意行为的行动。并且，与关键基础设施行业对口的政府机构对于可能受到恶意网络活动威胁的相关经济领域有着独特的洞察力。这些能力与美国情报共同体和国防部的专业知识可匹敌，反映了“整个政府层面”用来识别、减缓和防御网络事件及国家级事故的方法。

此外，政府已经落实了确保各部、局整合能力和资源，以有效、协调地应对恶意网络活动的机制。举个例子，在 2014 年，白宫开始使用网络响应组，即 CRG 来处理某些事件响应协调任务，这仿照了非常高效和长期存在的反恐安全组。CRG 专注于共享威胁信息、恶意软件签名、有关国家和非国家行为体的计划，并协调各政府部门之间的事件响应工作。恶意行为者越来越倾向于持破坏性的网络攻击目的侵入公共-私营网络。联邦政府视灵活的跨机构协调论坛，如 CRG，为政府反应能力的关键。通过建立 CRG 及类似机制，政府旨在共享变化中威胁和攻击信息，以及在更高层面协调政府开展事件响应的所有要素。

在采取“整个政府层面”的方法时，联邦政府正在努力为各部、局确立明确的责任，建立准实时态势感知所必要的沟通渠道，并加强政府与私营部门的接触，以便于各公司知道在面对网络威胁时该与谁接触。所有这些努力的目的是为了提高政府了解每次网络事件本质的能力，以及快速做出是否以及如何应对引起国家重大关切的网络事件的能力。

(2) 政策声明和战略通报

无论用什么威慑方法，要向即将或正在实施不可接受行为的敌人发出清晰和频繁的信号，这将增加美国成功威慑恶意网络活动的可能性。这种信号可以是直接或间接的，秘密或公开的。然而，美国必须保持一致、可靠的信息及信息传递渠道，并建立共享的态势感知能力，这样才能确定敌人是否正确接收并解读了信号。为此，整个政府层面同私营部门的咨询以及经常性的合作，加之国际协调，都增加了美国威慑行动中信号传递成功的可能性。

美国政策的一致传播对于建立一个能使盟友和敌人都理解美国的行为和含义的全球环境而言，是不可或缺的组成部分。政府的公开声明已经在试图解释美国在网络事务方面开展国际合作的观点，并强调了其重要性。在过去，美国已就关于以必要和合适方式应对网络威胁的意图做出了明确的声明。然而，在美国政府的声明中，关于响应的门槛、网络威胁后果的底线是模糊的，以防止敌人在底线以下进行恶意网络活动。政府将考虑是否更公开地谈论美国是否以

及如何应对恶意网络活动，尽管这样的公开讨论将需要谨慎平衡透明度以及情报和军事利益。

除了公开宣布的政策，美国也将利用战略通报作为一种威慑工具。在某些情况下，政府可能会突出调查、刑事指控、成功的检控或其他执法活动，以提高美国的威慑力。通过对这些案例的宣传，美国要确保恶意网络行为者知道其行为将招致巨大成本。美国政府还可以通过外交或其他渠道给外国对手发出警告，告之美国可以查到恶意网络活动的归属，并根据维护国家利益的需要应对网络攻击。在更极端的情况下，美国可能会加强这一战略消息的传递，并通过更有力的措施，包括更有力制裁或军事姿态，彰显我们的决心。

### （3）情报能力

情报收集、分析和行动是美国政府威慑网络威胁的关键。美国情报共同体的每个成员在确定最具威胁的网络敌人、其威胁目标（包括关键基础设施）、其决策心态及机会时，都起着关键的作用。为了加强这方面的工作，政府已经建立了网络威胁情报集成中心（CTIIC），便于把国家受到的外部网络威胁、影响影响美国利益的网络事件等关联起来。情报集成中心将支持美国政府中负责网络安全和网络防御的机构，也将推动和支持政府对外国网络威胁的打击。在履行其使命时，情报集成中心将为政府其他机构发现、调查以及抵御网络攻击及其他恶意网络活动起到关键的支撑作用。美国政府将继续运用其情报工作能力，以便最有效地保护美国的国家安全和经济安全，同时支持外交政策、保护隐私和公民自由、建立和维护公共信任。

### （4）国际接触

全世界都依赖互联的计算机系统，这应鼓励所有国家在共同的自身利益下合作，以制止网络威胁。针对网络威慑的有效国际合作需要美国同盟国和国际合作伙伴共享其对威胁环境的观点，牵头开发和宣传网络空间国家行为规范，并支持国际合作伙伴维护其自身网络安全。美国政府也正在与世界各地的同行合作，将网络防御、信息共享、事件响应和恢复领域的更紧密合作纳入双边和多边防务与安全关系，以增强威慑力。在采取这些行动的过程中，美国期望把志同道合的国家组合在一起，合力阻止网络攻击，增强全球经济安全，同时维护一个对所有用户开放和可互操作的全球互联网。

#### ①网络安全行为规范

正如同处在一个不断运动的世界中，对于什么级别的网络攻击可被认为是国际法下的武装攻击，国际上还没有形成共识。然而，美国已成功地建立了这样一个国际共识，即国际法，确实也适用于网络空间的国家行为。

在网络空间中，当有了具体的国家行为规范后，通过规范提供的背书或者遵循规范就可以进一步建立起相互信任，即国家间不会通过破坏力强大的网络攻击威胁彼此。这种规范还会使网络空间的行为标准实现社会化，符合每个国家的安全利益，同时也可形成对联合打击坏分子而言必不可少的国际支持。通过共同制定和执行这种规范，美国及其国际伙伴可以把潜在敌人隔离开来。美国政府已经确定了如下几个和平时期的网络空间行为规范，并将寻求对这些规范的国际支持：

- 一个国家不应实施或有意支持对关键基础设施进行蓄意破坏的在线行为，或者危害关键基础设施在提供对公共服务方面的用途。
- 一个国家不应实施或有意支持旨在阻止国家级 CSIRT（计算机安全事件响应小组）响应网络事件的行为，也不应利用 CSIRT 帮助在线活动意欲实施伤害。
- 一个国家应在接到另外国家的调查网络犯罪、收集电子证据、消除源自其本土的恶性

网络活动等协助请求时，以遵循其国内法和国际义务的方式进行合作。

- 一个国家不应实施或有意支持通过网络窃取知识产权来增强其公司或商务部门的竞争优势，包括商业机密或其他保密的商业信息。

#### ②促进国际社会的信任和透明，以及对合作伙伴的支持

通过国务院牵头的外交活动，司法部和联邦调查局牵头的执法合作伙伴关系，国土安全部和联邦调查局牵头的信息分享和事件响应伙伴关系，以及由国防部牵头的军事合作，美国政府努力扩大其与盟国和国际合作伙伴在网络事务上的紧密接触。美国与多个志同道合的国家，包括巴西、德国、印度、日本、韩国和中东、北欧和波罗的海等国家，举行了网络事务的“整个政府层面”的对话。必要时，我们也将继续与俄罗斯、中国和其他国家紧密接触，研究可行的网络安全合作和政策分歧对话机制。通过创建一种环境，使各方探讨新合作渠道，建立透明措施来减少网络事件误判风险，这样的对话强化了网络威慑方面的其他政策工作。由此，美国政府正在建造一个国际社区框架，使网络空间的行动能够抵消攻击意图。

减少网络空间某些方面的不确定性是这个框架的一个关键因素。在民族国家中，依靠恶意网络行为带来的非对称优势只会促使竞争，而不是合作。为了打击这种风险，并且为威慑创造必要的成功条件，美国政府正在寻求双边和多边的信任和透明度措施，以减少事件升级恶化和因对网络事件糟糕理解而造成不可预期后果的风险。美国正在国际上带领大家处理这些问题。政府在 2013 年 6 月与俄罗斯结束了首次双边网络信心建立措施的讨论，还在欧洲安全与合作组织内领导了制定第一套多边信心建立措施的工作。

信任不仅建立在这些战略接触上，还要通过计算机网络防护分析师之间的日常互动和合作来建立。这种互动增强了国家间的理解，并为国际合作伙伴如何看待网络空间、划分网络操作责任以及应对网络事件提供了真知灼见。日常工作，如计算机安全事件应急小组之间的合作和信息共享，则建立了合作关系和信任，为战略互信和透明度打下了基础。国土安全部和联邦调查局经常与国际合作伙伴共享感兴趣的事件信息，且在必要时共同调查并处理网络事件。很多部、局正在加大力量支持国土安全部的能力，使其与超过 200 多个国外的计算机安全事件响应小组共享网络防御信息，而且这些部、局还与很多这样的组织建立了合作关系。

#### （5）研究与开发

美国的敌人将继续开发绕过网络防御的新手段。为了跟上时代的步伐，美国政府必须发展创新性解决方案，使网络空间面对未来威胁有抵抗力。美国政府旨在通过整体规划和投资策略来塑造美国网络安全的未来，以开发必要的工具、技术和人力资源，这对不断提升美国的计算机、网络 and 关键基础设施的抵抗力并为威慑恶意网络行为提供新的技术选择而言必不可少。

政府正在对研究、开发、技术转移的优先级进行排序，通过消除入侵者在网络空间的优势来重塑安全格局，同时使网络空间更安全。政府投资的主要焦点是使硬件、软件、操作、交易、活动及商业行为在网络安全中天生就是安全的。举一个与此相关的例子，美国政府与私营部门合作实施了《网络空间可信身份国家战略》，它旨在用更安全、便捷和隐私增强的互联网服务访问方式来替换口令，这样做就减少了敌人可以用来侵入计算机和网络的一项关键漏洞。



## 5. 结论

30 年前，不会有人知道，信息在网络空间的自由流动会对创新和全球繁荣如此重要；也看不到，网络空间的恶意活动可以威胁公共安全和福利以及美国的国家安全和经济安全。这些威胁现在被广泛认识到了，而且同样清楚的是，它们仍将长期是美国面临的各种威胁的组成部分。各国政府、企业和个人对在线及数字服务的需求和应用持续增长，这将继续为那些可能对我们造成伤害的人提供有吸引力的目标。电信与计算机网络的融合、越来越多的对无线技术的使用、关键基础设施与互联网之间不断增长的互联等因素，为网络攻击创造了进一步的动因。在实现国家安全和外交政策目标的过程中，民族国家几乎肯定要继续把网络攻击及其他恶意网络活动作为一种非对称、事后可冠冕堂皇否认的选项。

美国政府致力于发现和抵御网络攻击及其他恶意网络活动，威慑那些实施此类行为的人。这个过程中，我们将使用所有必要和适当的国家权力工具，以保护我们的利益，并维持一个开放、互操作、安全、可靠的网络空间。一个可信的美国网络威慑需要政府所有部门持续努力来推行政策、发展能力，以改进网络防御水平、增强国家的网络韧性，并对加大恶意网络行为成本提供办法。这份政策文件为美国政府各部、局提供了一个初步的路线图，以明确其在美国网络威慑工作中的角色，使其执行特定的任务，并制定未来计划。

---

## 二十七、国防部网络战略

美国国防部

2015 年 4 月

---

1969 年，当国防部高级研究计划局（DARPA）的研究人员发明了当今互联网的前身时，他们无论如何也不会预料到这项发明会如此改变我们的世界。互联网最初只是科学家们用来共享信息的工具，现在却发展为由全球的计算机、系统和数据构成的庞大网络——我们称之为互联网。可以说，互联网连接了这个地球上几乎所有的人，成为创新和希望的引擎，为在全球范围内提供商品和服务，并为那些缺乏渠道的人带来了知识和理念。

美国依靠互联网与网络空间的系统和数据提供的一系列广泛的关键服务。这种依赖让我们所有人，包括个人、军队、商业、学校、政府，都处于网络攻击真实、危险的威胁之下。正如我们所看到的，现在国家、非国家的各种角色都在针对我们的网络和关键基础设施策划扰乱性和破坏性攻击，同时试图窃取美国的知识产权以削弱我们的技术和军事优势。

与美国其他政府机构一起，国防部负责保卫美国国土及利益免受攻击，包括网络空间可能发生的攻击。本战略是国防部第二个战略了，其目的是指导国防部发展网络力量，增强网络防护和震慑力。本战略聚焦国防部三项网络职能，建设网络能力和组织：一是捍卫国防部网络、系统和信息；二是捍卫美国土安全 and 国家利益，防御网络攻击，避免重大后果；三是支持军事行动和应急计划。

这是一项重要的职责，需要整个国防部以及美国政府其他支持性机构集中、长期的行动。作为一种管理和沟通的工具，这项战略将正确地引导对我们的力量进行投资、应对我们面临的威胁、完成我们的任务。这也为国防部设定了未来 5 年甚至更远期的更加清晰、明确的目标。我们寻求使我们的能力和计划对美国人民和整个世界更加透明、开放。

我将致力于该项战略的成功实施，并将肩负起达成目标所应承担的政府责任。在与我们的伙伴（包括美国政府、私营部门以及整个世界）的共同努力下，我们将更快、更好地建成能使我们在数字时代有效地保护美国及其利益的能力。

——美国国防部长 阿什顿·卡特

## 1. 引言

我们生活在网络世界。从金融交易到军事行动，企业和国家的一切活动都离不开网络空间。计算机代码模糊了网络与现实世界之间的界限，将数百万个对象连接到互联网或专用网络。电力公司依靠工业控制系统将电力输送到电网，航运管理人员利用卫星和互联网在全球海运航线上跟踪货物，美军依靠安全的网络和数据来执行任务。

美国致力于建立一个开放、安全、互动和可靠的互联网，以促进经济繁荣、公共安全以及商业和思想的自由流动。互联网的这些特点体现了美国核心价值观，即保护言论自由、公民隐私、创造力、机遇和创新精神。而这些特点已经让互联网为数十亿人提供了社会和经济价值。仅以美国经济为例，3%~13%的任何工商业增加值都来源于互联网相关业务。在过去的 10 年里，全球范围内网民增长了超过 20 亿人。然而，开放与活力在推动互联网迅速扩张的同时，也为危险的国家、非国家机构和人员提供了一种损害美国利益的手段。

在网络世界里，我们是脆弱的。今天，我们对数据保密性、可用性和完整性的依赖，与网络安全的不足形成鲜明对比。互联网最初的设计并未考虑安全性，而是作为一个开放的系统，使科学家和研究人员快速传输数据。如果没有对网络安全和网络防御进行大力投资，数据系统仍然是开放的，容易被人利用或受到攻击。出于经济或政治目的，恶意的利用网络空间窃取数据和知识产权。而尽管身处全球范围一个地区，攻击者仍可以利用网络直接打击远在千里之外的网络，破坏数据，扰乱企业或切断关键系统。

国家和非国家角色（包括机构或个人）实施网络操作来实现各种政治、经济和军事。他们可能会打击一个国家的价值体系以及其利益或诉求。例如，某国对索尼影业的攻击是迄今为止美国机构受到的最具破坏性的网络攻击之一。这次袭击进一步刺激了全国范围内有关网络威胁的性质以及是否需要改善网络安全的讨论。

在国际关系中，将网络攻击不断作为政治手段来使用是一个危险的趋势。脆弱的数据系统为国家和非国家角色打击美国及其利益，提供了绝佳机会。美国国防部认为，在冲突期间，潜在敌人将通过攻击美国或盟国的关键基础设施和军用网络来获得战略优势。除了上述的攻击，有经验的攻击者可以针对公用事业工业控制系统（ICS）发动攻击以影响公共安全，或进入网络来操作公民健康记录，影响个人利益。如果一次具有破坏性、操控性或摧毁性的网络攻击造成生命损失、财产被毁、政策目标受到伤害或经济利益受到影响，将给美国经济和国家安全带来严重风险。

领导人必须采取措施，以减轻网络风险。各国政府、企业和组织机构必须仔细考虑它们需要保护的系统和数据的优先顺序，评估风险和危害，并在网络安全和网络防御能力上进行谨慎投资，以实现其安全目的和目标。在这些网络防御投资的背后，各组织必须制定业务连续性计划并为在降级的网络环境（即网络和数据访问变得不稳定）下运行做好准备。为了降低网络空间风险性，需要制定综合应对战略，并且必要时能够承受毁灭性和破坏性的攻击。

### 在网络空间保卫美国

美国国防部协同其他机构共同负责保护美国本土和美国利益免受攻击，包括可能发生在网络空间的攻击。不论是在平时、危机或冲突时，国防部遵循美国和国际法律，致力于阻止攻击，

抵御那些试图伤害美国利益的敌人。为此，国防部建立了网络作战能力，并正在将这些能力集成到美国政府用来捍卫国家利益的完整工具集中，其中包括外交、信息、军事、经济、金融和执法工具。

2011年5月发布了《国防部网络空间行动战略》，在过去的4年里，该战略为国防部的网络活动和行动提供了指导，以支持美国的国家利益。本战略则针对在未来5年中需实现的国防部网络活动和任务，提出了优先战略目的和目标。本战略着眼于保护国防部网络、系统和信息，保护国家不因网络攻击受到严重影响，支持（作战）行动和应急计划。按照有关国防部网络任务部队和网络人才的既有决策，本战略为减轻预期风险以及抓住机会提高美国的国家安全，提供了新的和更为具体的指导。

作为一项基本原则，网络安全是美国联邦政府作为一个团队的工作。为完成使命，国防部必须联合其他部门和机构、国际盟友和伙伴、州和地方政府，并且最重要的是与私营部门建立合作伙伴关系。

### 网络安全活动

为支援网络空间任务，在网络空间之外，国防部开展了系列活动以改善整体网络安全态势并保护美国利益。例如，国防部配合美国政府的机构，与私营部门以及我们的国际伙伴共享信息，建立联盟和伙伴关系，并促进规范的负责任的行为，提高全球战略稳定性。

- 推动信息共享和机构之间的协调：为了保护和推动美国在网络空间的利益发展，国防部就多项网络活动与美国政府机构共享信息并加强综合协调。举例来说，如果国防部获悉了某些恶意网络活动可能会影响到关系美国国家安全、经济安全或公共安全的重要网络与信息系统，由于国土安全部（DHS）、联邦调查局（FBI）等机构可以接触到美国的实体机构并且时常涉及其他国家，国防部将向这些机构提供支持，共享威胁信息，如某潜在攻击的技术指标。这样的信息共享可以明显提高组织机构应对各类网络攻击的能力。除了共享信息，国防部还与美国政府其他机构建立了合作伙伴关系以同步行动，并分享经验教训和网络安全最佳实践，包括事件管理和网络防御反应。
- 向私营部门搭建桥梁：从应用程序开发商到互联网服务提供商，私营公司提供了构建网络空间的各种产品和服务。国防部依靠私营部门建立自身网络，提供网络安全服务以及研究和开发高级功能。在其整个发展历史中，国防部得益于私营部门的创新。展望未来，国防部将与私营部门密切协作，验证本部门有关网络安全的新思路并将其商业化。
- 建立海外联盟、同盟和伙伴关系：国防部参与了大量活动以提高海外网络安全和网络作战能力。国防部帮助了美国盟友和合作伙伴，使其了解他们所面临的网络威胁，并建立了保护其网络和数据的必要能力。同样地，盟友和合作伙伴也经常互补性地帮助美国提高相关能力，美国寻求建立强大的联盟和同盟来对抗潜在敌人的网络活动。从战略上讲，一个统一的联盟将传递这样的信息，即美国及其盟友与伙伴处于集体防御状态。除了五眼联盟，国防部与中东、亚太和欧洲的主要合作伙伴密切合作，了解网络安全环境并建立网络防御能力。

### 网络空间三项主要职能

总统已经确立了治理网络行动的原则和流程。这些原则和流程的目的是规划、开发和有效利用我们的能力，并确保这些网络行动符合美国在国内和国际上推广的价值观。

国防部在网络空间主要有以下三项职能。

(1) 必须保卫自身网络、系统和信息。美军在作战方面对网络空间的依赖，促使国防部长在 2011 年宣布将网络空间作为作战领域，以组织、训练和装备美军。国防部必须能够保护自己的网络免遭攻击，并在安全措施失败后能够迅速恢复。因此，为保证国防部信息网络部（DoDIN）安全运行，国防部在现有工作基础上实施网络防御行动。在其网络内发现恶意活动时，国防部具备快速反应能力以关闭或缩小脆弱性，保护其网络和系统。针对国防部网络的网络防御行动在国防部网络空间行动中占据了绝大部分。

除了国防投资，国防部必须准备好在网络空间访问受阻的环境下实施行动。在冷战期间，部队必须为在可能被敌人使用先进技术中断通信的环境下行动做好准备，包括使用电磁脉冲扰乱卫星和其他全球通信能力。指挥员定期进行训练，要求自己的团队在无法访问通信系统的条件下行动。通过多年的实践与锻炼，韧性文化植根于军方，各部队都可以在恶劣环境下作战。

然而，冷战结束后，年青一代已经越来越习惯于互联环境。冷战后成长起来男女军人更习惯于获取信息和通信，信息革命使部队更加敏捷，全球适应力更强。在不断升级的网络威胁面前，前几代的教训必须向下传递。国防部必须能够履行其保卫国家的使命。组织机构必须锻炼和学习在没有工具的情况下开展行动，尽管这些工具已经成为它们日常生活和行动的一个重要组成部分。

(2) 必须做好准备，保卫国家及其利益不因网络攻击受到严重影响。虽然总统和美国国家安全团队根据具体案件和实际情况对网络攻击进行评估，但严重的后果可能包括生命损失、财产大量受损，严重影响美国外交政策或经济。

如果由总统或国防部长指挥，美军可以发动网络战来对抗在网络空间即将或正在进行的对美国本土或美国利益的攻击活动。这样的防御措施是为了挫败攻击，防止破坏财产和导致生命损失。国防部试图将其能力与其他政府机构同步，制定一套方案和方法来阻止大规模网络攻击，包括执法、情报和外交工具。作为一个原则问题，美国在发动网络战之前，将寻求所有网络防御和执法方案，以减轻针对美国本土或美国利益的任何潜在网络风险。

美国政府在保卫国家免受严重网络攻击上发挥了有限和特定的作用。私营部门拥有并经营着超过 90% 的网络和网络基础设施，因此是防御的第一道防线。其中改善美国的整体网络安全态势的一个最重要的步骤是，公司优先考虑它们必须保护的网络和数据，并投资提高自身的网络安全。尽管美国政府必须准备保卫国家应对最危险的攻击，但大部分入侵活动都可以通过比较基本的网络安全投资来解决，企业可以而且必须开展这方面的投资。

(3) 如果由总统或国防部长直接指挥，国防部必须能够支持军事行动和应急计划提供综合网络能力。有时，总统或国防部长可能会决定，需要实施网络战来破坏对手的军事相关的网络或基础设施，使美军能够在地区作战中保护美国利益。例如，美国军方可能会使用网络操作终止针对美国的冲突，或破坏对手的军事系统，以防止使用武力对付美国的利益。在适当时，美国网络司令部（USCYBERCOM）也能协同其他美国政府机构一起指挥网络战，以阻止或挫败其他领域的战略威胁。

为了确保互联网保持开放、安全和繁荣，美国网络行动将遵循克制原则，以保护生命、防止破坏财产为需要。在其他行动领域，国防部在网络空间将尊重美国长期以来的价值观，包括支持法治，尊重和保护言论自由、隐私权以及信息、贸易和思想的自由流动。任何有关在国防部网络之外进行的网络行动的决定，都是经仔细和慎重考虑，在严格的政策和运行监督下并

按照武装冲突法做出的。因为它在建立网络能力以保卫美国的国家利益进行投资，国防部总是慎重考虑国家和非国家角色的行为对国防政策的潜在影响。

### 新型网络任务部队

为了履行其任务和执行这一战略，国防部需要国防部和更广泛的美国政府机构的多位领导和组织的承诺与协调。国防部执法、情报、反间谍和政策组织都发挥着积极的作用，每位建立和运营国防部的网络和信息技术系统的男性和女性都起到了积极的作用。每个组织都需要发挥自己的作用。例如，整个国防部的网络服务提供商必须适应和积极遵循网络安全的最佳实践和网络防御令。美国网络司令部必须与其他国防部组织同步其活动，特别是作战司令部，以应对新出现的挑战和机遇。安装网络的所有者和运营商必须与军事部门的计算机应急响应小组（CERT）、国土安全部和美国网络司令部建立合作伙伴，依靠关键任务系统和支持它们的民用系统制定适应性防御和连续性计划。要取得成功就需要在部门内和机构间建立有创造性的和强大的合作伙伴关系。

在国防部的网络人才和力量中，网络任务部队（CMF）发挥了独特的作用。在 2012 年，国防部开始组建网络任务部队以执行国防部的网络任务。一旦全面投入使用，网络任务部队将包括近 6 200 名来自全国各地的军事部门和国防相关机构的军人、非军人和承包商。该网络任务部队由国防部和美国政府共同开展的一项主要投资，本战略核心目标是设置特定的目的和目标，引导网络任务部队和国防部的更为广泛的网络人才的发展，以保护和捍卫美国的国家利益。

网络任务部队将包括 133 个网络行动组，主要列举如下：网络保护部队将致力于增强传统防御措施，重点保卫国防部高优先级的网络和系统免受并高优先级的威胁；国家任务部队及其相关支持团队将捍卫美国及其利益不因网络攻击受到严重影响；作战任务部队及其相关支持团队将支持作战指挥部，通过综合性的网络空间效果来支持运行计划和应急行动；作战指挥部将作战任务部队和网络保护小组加入计划和行动中，在网络空间雇用它们，而国家任务部队受美国网络司令部指挥。在这个体系之外，团队还可以支持部门所要求的其他任务。

从 2013 年开始，国防部开始将 CMF 整合到更大的多任务美军部队中以实现跨域协同，确保 CMF 在部队内部就绪，并重组了军用和民用劳动力和基础设施来执行国防部的任务。在实施这一战略的过程中，国防部将继续打造 CMF，并不断发展所需的指挥、控制，以及使组织有效运作。国防部将重点确保对其部队针对网络作战能力进行培训并准备好使用各种能力和体系进行操作，继续建设政策和法律框架来管理 CMF 人员，以及将 CMF 融入国防部的总体规划和人员发展计划中。

这一战略认识到，有效的网络安全需要在国防部内部以及与整个联邦政府行业、国际盟友和合作伙伴，与州和地方政府开展密切合作。由于利益相关者数量和多样性、信息跨国界流动以及相关职责、权限和能力跨越政府和私营部门，实现安全的网络空间需要政府和国际上广泛参与。对于每个国防部的任务，国防部都必须继续制定协调其网络业务的日常关系和流程。

这一新战略考虑了具体的风险和机遇。例如，美国国防部自己的网络是世界各地成千上万的网络拼凑而成的，而国防部缺乏一个可视的组织化架构来有效地保护其分布的网络。国防部必须进一步开发足以发现敌人意图和能力的预警情报系统，排除针对国防部和美国的破坏及毁灭性网络攻击。除了自身的网络，国防部在美国和海外行动中也要依靠民用关键基础设施，然而这样的关键基础设施的网络安全是不确定的。

为了减轻上述和其他风险，提高美国国家安全，本战略设置了国防部要实现的战略目的，并规定了每个目的对应目标和指标。所有这些战略中的目的和目标都反映了 2015 年美国国家安全战略和 2014 年四年防务评估报告提出的目标。

国防部设定了 5 项网络空间战略性目的，包括：

- (1) 建立并巩固现有力量和能力，为实施网络空间行动做好准备。
- (2) 保护国防部信息网络，保证国防部数据安全，降低国防部数据和任务面临的风险。
- (3) 为保卫美国本土及关键利益做好准备，防止扰乱性或破坏性的网络攻击造成严重后果。
- (4) 建立并维护可行的网络空间方案，制定实施计划以控制冲突升级，在各层次改变冲突环境。
- (5) 建立并保持强有力的国际联盟和伙伴关系，以防止共同风险，提高国际安全与稳定。

## 2. 战略内容

战略内容包括四个方面：主要的网络威胁、恶意软件扩散、国防部网络和基础设施面临的风险、威慑未来安全环境（快速响应、拒绝攻击、可恢复性强）。

### 关键的网络威胁

2013—2015 年，国家情报主任将网络威胁列为美国的头号战略威胁，自 2001 年 9 月 11 日起首次将它放在恐怖主义之前。潜在的国家和非国家敌人针对美国全球利益发动恶意攻击，挑战了美国和国际社会的容忍极限。攻击者出于各种原因攻入美国的网络和系统，如窃取知识产权、扰乱企业运营达到激进目的，或通过发动破坏性和毁灭性攻击来实现军事目标。

我们潜在敌人已经开始大力投资网络空间，这是由于网络空间为之提供了一种切实可行的、理论上不可否认的能力，足以威胁美国土安全和损害美国利益。一些国家已经具备了先进的网络能力和战略。

除了国家威胁，非国家角色，如伊拉克和黎凡特的伊斯兰国（ISIL）使用网络空间招募战士和传播宣传，并宣布它们有意收购颠覆性和破坏性的网络功能。犯罪者在网络空间构成了相当的威胁，特别是对金融机构，以及意识形态群体经常使用黑客以推动他们的政治目的。国家和非国家威胁往往还糅合在一起，爱国机构经常为国家和非国家实体充当了网络代理人，以掩护国家实施者。这种行为使溯源更加困难，并增加了误判的可能性。

### 恶意软件扩散

恶意代码或软件（恶意软件）全球的扩散增大了美国网络和数据面临的风险。针对军事系统或工业控制系统发动破坏性或毁灭性的网络行动需要专业知识，但一个潜在敌人并不需要花费数十亿美元来开发攻击能力。一个民族或国家、非国家团体甚至个人角色都可以在黑市上购买具有破坏性的恶意软件和其他功能。国家和非国家角色也要花钱请专家来寻找漏洞并制定攻击方案。这种做法已经创造了一个危险的和不可控的市场，涉及国际体系中多个角色，往往是出于竞争目的。随着时间发展，网络能力更加容易获得，美国国防部评估认为，国家和非国家行为者将继续寻求和发展网络战能力来对付美国。



## 国防部网络和基础设施面临的风险

国防部自身的网络和系统很容易受到入侵和攻击。除了国防部自己的网络，国防部还需要依靠关键基础设施和重要资源来实施行动，针对这些基础设施和资源的网络攻击，可能会影响美军应急作战能力。国防部已经取得一定进展，通过其任务保证计划确定了自身关键资产的网络脆弱性，包括针对很多关键资产确定了重要物理资产所依赖的物理网络基础设施，但必须采取更多措施来保护国防部的网络基础设施。

除了破坏性和毁坏性攻击，网络角色还窃取了大量美国政府和商业实体的业务信息和知识产权，这也会影响国防部。受害者包括武器开发商以及为美国运输司令部（USTRANSCOM）进行武力运输提供服务的商业公司。国家行为者窃取了美国国防部的知识产权，以削弱美国的战略和技术优势，并使它们自己的军事和经济发展获利。

最后，国防部面临来自美国政府持续预算不确定的风险。虽然国防部在预算分配已将资源优先用于开发网络战能力，长期财政不确定性就要求国防部在整理预算缩减的情况下计划如何打造其网络能力。国防部必须继续优先考虑其网络投资并发展在国内外保卫美国利益所需要的能力。

## 未来安全环境下的威慑

在不断升级的威胁面前，国防部必须致力于制定和实施全面网络威慑战略，以阻止主要的国家和非国家角色对美国利益实施网络攻击。由于网络空间国家和非国家网络角色及相关可用的破坏性网络工具的种类和数量众多，有效的威慑战略需要一系列足以影响国家或非国家角色行为的政策和能力。

美国国防部建立了自己的网络任务部队和整体能力，国防部假定要对通过网络攻击威胁美国利益的行为形成威慑力，但仅通过网络政策不可能实现，它需要我们各方面的行动，其中包括宣示政策、实质性迹象发现和预警能力、防御态势、有效的响应程序以及美国网络和系统的整体可恢复性。因此，国家和非国家组织在网络空间的威慑力将需要多个美国政府部门和机构的共同聚焦。国防部在这一问题上发挥着若干特定的角色。

某种程度上，威慑是一种感知功能。它的工作原理是说服潜在敌人认识到，如果对美国进行攻击将遭受无法接受的损失，并降低潜在敌人成功攻击的可能性。美国必须能够声明或显示有效的响应能力，震慑对手不敢发起攻击，开发能够拒绝潜在攻击有效的防御能力，并且如果攻击穿透了美国的防御体系，加强美国信息系统承受攻击的整体韧性。此外，美国需要强大的情报、取证、迹象发现和预警能力，降低网络空间的匿名性，在溯源方面提高信心。

- 响应：美国已经明确表示将通过其防御能力应对关乎美国利益的网络攻击。美国已多次阐明这项宣示性政策，包括 2011 年的《美国网络空间国际战略》、2011 年国防部向国会提交的网络政策报告以及通过总统和国防部长的公开声明。美国将继续以我们选择的时间、方式和地点，应对关乎美国利益的网络攻击适当地使用美国武力手段并根据适用法律。
- 拒绝：虽然国防部在成立网络任务部队上取得进展，国防部必须提高其防御能力，以保卫国防部网络和国家免受极其复杂的网络攻击，必须与其他部门、机构、国际盟友和合作伙伴以及私营部门合作改善网络安全，通过抗拒攻击增强威慑力。
- 韧性：由于国防部的能力不一定能保证每个网络攻击都被成功阻拦，国防部必须投资

于韧性和冗余系统，使国防部网络即使遭受了破坏性或毁坏性网络攻击，仍能继续运行。但是，国防部不能为其职权以外的组织建立韧性能力。为了使韧性成为有效威慑力的一个成功因素，政府其他机构必须与关键基础设施的所有者、运营者和私营部门开展更为广泛的合作开发可以抵御潜在攻击的韧性和冗余系统。有效抗御措施可以帮助说服美国的潜在敌人，对美国网络和系统发动网络攻击是徒劳无益的。

由于网络空间的匿名特性，国家和非国家团体都有可能实施恶意网络活动，溯源是使网络威慑战略有效的一个基本要素。在情报、溯源和警示方面，国防部和情报机构已经在来源收集、分析和传播方面更大力投入，所有这些努力都希望在网络空间降低国家和非国家行为者活动的匿名性。情报和溯源能力有助于揭开网络空间的角色，找出攻击源，并确定战术、技术和程序。溯源使国防部或其他机构能够对到来的网络攻击做出回应和反抗措施。

首先，对公共组织和个人的溯源可以在阻止网络上的角色发动网络攻击方面发挥重要作用。在溯源方面，国防部将继续与私营部门和美国政府其他机构开展密切合作。随着时间的推移，这项工作对于威慑激进组织、犯罪组织以及需要先进网络能力的其他角色来说将显得尤其重要。

其次，网络战能力为国家和非国家行为者损害美国利益提供了一种方式，这种方式可能或未必需要纯粹的军事响应，但仍然可以显著威胁到美国的国家安全并需要某种形式的非军事响应。为了应对某些攻击和入侵，美国可能会采取外交行动，采取执法行动，并考虑经济制裁。

### 3. 战略目标

为了在当前和未来的安全环境降低风险并保护美国利益，美国国防部概述了其活动和任务的5个战略目的及具体目标。

(1) 目标 1：建立并维护现有力量和能力，为实施网络空间行动做好准备。

为在网络空间有效运作，国防部需要受过严格训练、准备就绪并装备一流技术能力的部队和人员。在 2013 年美国国防部通过启动网络任务部队（CMF），开始在其网络人员和技术上进行重大投资。现在，国防部必须用好这项投资来进行人员培训，建立有效的组织、指挥与控制系统，以及全面发展国防部网络行动所需要的能力。本战略提出了国防部在未来 5 年或更长时间内有关招募、训练及装备其部队与人员的具体目标。

(2) 目标 2：捍卫国防部信息网络，保证国防部数据安全，降低国防部数据和任务面临的风险。

由于国防部整个网络的攻击面太大，难以关闭所有漏洞，无法做到保护每个网络和系统免受各种入侵，国防部必须采取措施来标识、优先处理并保卫其最重要的网络和数据，以便它可以有效执行任务。国防部还必须规划和演练，当国防部的网络和数据受到攻击或当网络环境受到攻击，或者国防部赖以运行的关键基础设施及应急计划被打乱时的情境。

最后，国防部必须提高技术和创新的屏障，使其网络防御能力领先于网络威胁，包括在联合信息环境（JIE）建设方面并采用防御能力更强的网络架构。在国防部网络之外，国防部必须与私营部门合作，以帮助保护国防工业基础贸易数据，并准备协助其他机构强化美国的网络和数据免受网络攻击和网络间谍活动影响。

(3) 目标 3：为保卫美国本土及关键利益做好准备，防御扰乱性或破坏性的网络攻击，避

免造成严重后果。

国防部必须与其跨部门伙伴间、私营部门、盟国和伙伴国加强合作，以威慑并在必要时击败网络攻击，防止对美国本土和美国的利益造成严重后果。国防部必须开发其情报、预警和运营能力，以在产生实际效果前减少复杂、恶意的网络攻击。符合所有适用法律和政策，国防部需要对全球的网络和系统、敌人的能力以及恶意软件操盘手和市场掌握精准、具体、预知和可操作的情报。为了保卫国家，国防部必须与政府其他机构建立伙伴关系以准备进行联合网络作战来威慑或击败网络入侵。国防部正在着力构建实现这一任务的必要功能、流程和计划。

(4) 目标 4：建立并维护可行的网络空间方案，制定实施计划以控制冲突升级，在各个阶段改变冲突环境。

在高度紧张或完全敌对行动中，国防部必须能够为总统控制冲突升级提供多个选项。必要时，国防部应该能够通过网络战来扰乱敌人的指挥和控制网络、与军事有关的关键基础设施和武器能力。作为美国使用的全方位工具的一部分，国防部必须制定可行的网络方案并将这些方案集成到部门计划中。国防部将开发网络功能以准确实现关键性安全目标，并最大程度地减少生命和财产损失。为确保工作的统一性，国防部将指定作战司令部来计划网络战，并使其与各个领域的军事行动保持同步。

(5) 目标 5：建立并维护强有力的国际联盟和合作伙伴关系，以防止共同风险，提高国际安全与稳定。

国防部的 3 个主要网络任务都需要与国外的盟友和伙伴密切合作。在参与国际网络活动时，美国国防部寻求建立网络安全和网络防御伙伴关系能力，并在适当情况下深化业务伙伴关系。

由于网络资源的高需求和相对稀缺性，国防部必须做出艰难选择，并将伙伴关系能力举措集中在关乎重要国家利益的领域上。在未来 5 年中，除了正在进行在其他地区的合作伙伴能力建设，美国国防部将把国际合作重点放在中东、亚太和重点北约盟国。随着这一战略的实施，国防部将不断评估国际环境，发展创新型伙伴关系，以应对新出现的挑战和机遇。

## 4. 实现目标

每项国防部战略目的都需要通过若干具体、可衡量的目标来实现。国防部长首席网络顾问办公室，采办、技术和后勤助理部长办公室以及联合参谋部将与国防部各内设部门将优先执行并监督这一战略及其目标，安排主要和辅助责任办公室来管理每个目标。主要责任办公室将针对各个目标制定项目计划，首席网络顾问负责追踪每个战略目标的进展，直至战略目的最终得以成功实现。

### 实现目标 1

建立并维护现有力量和能力，为实施网络空间行动做好准备。

- 建立网络人才力量。为用好对国防部在网络人才方面的重要投资并帮助实现这一战略的多个目标，美国国防部的首要任务是建立一个可以立即投入使用的网络任务部队和相关的网络队伍。该工作队伍的建立基于 3 个支柱：强化训练，完善军民人员招募、保留人才，以及来自私营部门的更强有力的支持。

- 保持长期的训练环境。国防部需要对个人和集体的能力进行训练来实现这一战略提出的目标并满足未来的作战需求。美国网络司令部将协同其他内设部门、机构和军事部门来确定相关要求并创建一个训练环境，使得全部网络力量可以针对跨边界和跨网络任务开展联合培训（包括训练和任务演练）、试验、认证，以及对网络的能力和战术、技术和程序进行评估和研发。
- 建立可行的职业发展道路。纵观本战略，并按照 2013 年网络任务部队（CMF）决策，国防部将继续为所有执行和支持网络行动的军事人员提供可行的职业发展道路。
- 吸收国民警卫队和预备役。贯彻这一战略的过程中，国防部将借鉴国民警卫队和预备役的专业知识资源，促进可以创造性地解决网络安全问题。预备役为支持国防部的任务提供了特有功能，包括参加国防工业基地和商务部门。它代表了美国国防部有关网络响应的关键增长能力。
- 改进非军事人员招聘和人才保留机制。除了培养高技能军人，国防部必须招聘和留住高技能非军事人员，包括网络大军中的技术人员。非军事人员必须遵循一个良好的职业发展和提升轨迹，并使其具备最佳的发展和成功机会。
- 制定和实施与私营部门的交流计划。为了扩充国防部民间网络大军，国防部必须能够从全国最好的网络安全和信息技术公司聘请专业技术专家，发挥特定工程和分析的作用。国防部将与私营部门成功开展交流，并为针对国防部的网络空间任务设计和开发新作战概念带来实际效益。
- 支持国家网络空间教育计划。国防部将制定相关政策，以支持国家网络安全教育计划。协同机构间合作伙伴、一个或多个教育机构以及国家和私营合作伙伴，国防部将继续投入在网络安全和网络防御技术和政策方面培养创新型人才。
- 建立网络战技术能力。在 2013 年，美国国防部开发了一个模型，可以有效建立网络任务部队（CMF）并为向总统及国防部长提供可行的网络军事方案。国防部必须通过技术手段为作战司令部的任务提供网络行动支持。主要措施包括以下内容：
  - 开发统一平台。在规划要求的基础上，国防部将针对不同网络平台的整合，针对可互操作和可扩展的网络，提出网络能力建设的详细要求。这个统一的平台将使网络任务部队（CMF）按照国家的要求来开展全方面网空行动。
  - 加快研究和开发工作。国防部将继续加快研究和开发创新型网络的工作以建设网络能力。美国国防部的研究和开发团队以及已建立和新兴的私营部门合作伙伴可以提供国防部和美国在开发领先技术上具有显著优势，以保护美国在网络空间的利益。除了支持现有的和计划性投资，国防部将侧重关于开发网络功能的基础研究和应用研究，以拓展网络任务部队（CMF）及更广泛的国防部网络队伍的能力。
- 验证并继续完善网络战的自适应指挥和控制机制。最近几年，国防部围绕其 3 项主要任务，在建立指挥和控制模式上取得显著进展，但其指挥和控制模式必须是确定的，资源充分并且经过测试的，以确保其有效性。指挥和控制模型应服务于美国网络司令部和作战司令部。它必须是高效实用的，而且必须促进 3 个网络任务工作的统一性。
- 建立企业范围内的网络建模和仿真能力。国防部将协同情报机构开发用来评估网络作战效能的数据架构、数据库、算法以及建模和仿真（M&S）的能力。

- 评估网络任务部队的能力。对未来网络任务部队在面临多个突发情况时实现其任务目标的能力进行评估。
  - 联合参谋部由美国网络司令部和国防部内设部门提供支持，将为首席网络顾问提出、收集、分析并报告一套合适的衡量标准，用来衡量网络任务部队（CMF）的作战能力。这些指标将包括美国网络司令部应变能力的状态更新，包括开发能力和熟练程度，以及应急情况下可能需要的访问和工具。鉴于这一分析，国防部将制定计划用于确保网络任务部队具有适当的能力和灵活性，能够响应战略环境的变化。

## 实现目标 2

捍卫国防部信息网络，保证国防部数据安全，降低国防部数据和任务面临的风险。

- 建立联合信息环境（JIE）单一安全架构。国防部将建立国防部信息网络，以满足联合信息环境的单一安全架构。单一安全架构将适应和发展，以减轻网络威胁。这将有助于美国国防部开发并遵循最佳网络安全实践和，它的小网络覆盖将允许美国网络司令部、作战司令部和国防部内设部门维护有关网络的威胁和缓解的全面态势感知能力。
  - 联合信息环境的单一安全架构有助于强大的网络防御能力，从保护服务特定的网络和系统转移到按照统一的方式保护国防部网络。联合信息环境的单一安全架构必须具有增强网络态势感知能力，按验证要求进行部署，并能适应未来的防御措施。
  - 作为联合信息环境规划的一部分，国防部将设计一个框架以开发新的防御技术并将其集成美国国防部的网络安全体系结构中，包括基于异常的检测能力，通过数据分析找出漏洞和威胁以及先进的加密方法。
- 评估和确保国防部信息网络（DoDIN）联合部队总部行动的有效性。运行在美国网络司令部之下，国防部信息网络联合部队总部将协调国防部作战和任务的网络防御并减少网络风险。国防部将评估、验证和全面落实国防部信息网络联合部队总部决策以保护国防部网络安全运行，并缓解国防部的任务面临的网络风险。
- 减少已知的漏洞。国防部将实施措施来减少已知漏洞，这些漏洞给美国国防部的网络和数据带了很高的风险。除了零日漏洞，国防部网络和系统面临的最大威胁之一就是已知的高风险安全漏洞，这些安全漏洞可以被潜在敌人利用。国防部经常发现一旦敌人入侵系统才急于关闭安全漏洞。国防部首席信息官（CIO）将带领实现分发软件和配置的补丁、更新和修复的自动化的补丁管理功能，以减少威胁美国国防部的网络和系统的已知的主要漏洞。
- 评估国防部网络防御力量。国防部会评估其网络防御部队在综合、自适应和动态防御作战方面的能力。企业级和网络保护小组（CPT）的网络防御者必须能够发现、检测、分析和缓解威胁和脆弱性，以保护美国国防部信息网络。
- 改善当前国防部计算机网络防御服务供应商（CNDSP）体系在捍卫和保护国防部网络上的有效性。计算机网络防御服务提供商为国防部网络提供网络安全解决方案，包括监测、检测和防护能力。国防部将决定当前 CNDSP 流程是否足以对抗网络空间已知和预计的威胁，以及是否目前 CNDSP 力量得到充分的训练和装备，以对抗高级威胁。最后，国防部将决定其 CNDSP 力量是否能融入更广泛的网络空间的指挥和控制架构中，以及综合架构在面临泛 CNDSP 和 CPT 保护网络和数据s的网络威胁时如何发挥作用。

- 规划网络防御和抗灾能力。国防部必须标识支撑国防部关键任务的网络并制定保护计划。国防部必须通过仔细评估它必须保护的、优先级高的资产，以确保国防部相应开展任务和进行演练。
  - 将网络纳入任务保证评估。美国国防部将网络安全要求和评估纳入国防部任务保证计划并适当更新国防部的政策。目前，美国国防部内设部门采取了不同的方法为任务保证衡量和评估网络风险。国防部将建立一个联合任务保证评估计划，其中包括有关网络安全评估、网络安全要求以及网络运营需求的整合。
  - 评估网络保护小组（CPT）的能力。国防部将针对按照作战司令部要求设定的任务保证优先级，对 CPT 容量、能力和工作模式进行评估。
  - 提高武器系统的网络安全。国防部将基于业务需求，评估并启动改进当前和未来武器系统的网络安全性。对于所有美国国防部未来获取或采购的武器系统，国防部将要求武器系统满足强制性网络安全标准。获取和采购政策和做法将被更新以提升整个系统生命周期网络安全的有效性。
  - 建立并实行连续性计划。所有国防部内设部门将确定发生网络中断和降级事件时最关键业务并建立韧性计划保持业务连续性。军事行动计划必须充分结合在受损的网络环境中运行的能力。军队必须演练能够在网络和数据访问不确定的受损的网络环境下开展军事行动。各部门必须有效地平衡网络风险，以确保能够在物理世界继续执行任务。
- 国防部的网络防御红队。国防部已经发展成熟的红队检测重要网络和任务系统中漏洞的能力，并更好地准备其网络防御部队。展望未来，国防部必须将红队的能力聚焦在优先级高的网络和任务系统上，以确保国防部能够执行最关键任务。作为这项工作的一部分，国防部每项主要演练都应包括网络红队，在针对国防部行动被敌人破坏时的模拟情况下测试国防部网络防御能力。各部门将被定期审计，以确保跟进将红队的调查结果，并改善其网络安全态势。
- 减少内部威胁的风险。一个国家的国防依赖于那些掌握着国家秘密的人员的忠诚度。国防部已投资于必要的技术和人员解决方案，以在对美国的安全造成影响前发现威胁。国防部通过持续的网络监控、改进的人员网络安全培训以及发现、报告和跟踪可疑行为的方法来继续部署和实施这些解决方案。
  - 这项工作超出了信息技术的范围，包括人员和可靠性的问题。减少内部威胁，需要对人员有良好的领导力和问责机制。除了执行政策和协议，领导者将努力创造感知文化，在威胁后果发生前预见、发现和应对内部威胁。
- 针对为非军事政府机构提供国防支持进行演练。根据现有的和规划的部队结构，国防部将制定一个框架，并行使国防支援民事局（DSCA）能力对国土安全部和其他机构提供支持，并在收到指令时与国家和地方当局一起帮助在紧急状况下保护联邦政府和私营部门。
  - 美国国防部的年度演习方案涉及网络防护，将包括与美国国土安全部和联邦调查局进行应急演练，可能需要在合作伙伴机构的领导下，紧急调动人力帮助保护关键基础设施。该框架将介绍作战司令部和作战支援机构如何与国土安全部和联邦调查局及其他机构开展合作，以提高集成、演练和支持能力。

- 界定和完善国民警卫队的作用，以支持执法、保卫国土、和支持非军事政府机构任务。国防部将与国民警卫队一起明确国民警卫队协调、培训、建议和辅助（C/TAA）的作用，通过网络防护 16-1 细化实施。根据其现有的和规划的部队结构，国民警卫队将发挥协调、培训、咨询，协助州和地方机构以及国内关键基础设施，并向执法机构，国土防御机构以及民事当局有关支持国家目标的活动防御提供支持。
- 改进国防部和 DIB 数据保护的问责制和责任。国防部将确保政策和任何相关的联邦规则或合同要求已经落实，要求 DIB 企业向国防网络犯罪中心上报数据盗窃和丢失情况。
  - 国防部将继续评估国防联邦采购条例补充（DFARS）规则和相关的指导，以确保它们逐步完善，按照公认标准和国家标准与技术研究院（NIST）发布的标准保护数据免受对手攻击。
  - 国防部将继续推动公司参与威胁信息共享计划，如网络安全/信息安全保障计划。
  - 随着 DIB 认证机构清理了国防承包商的网站，国防安全服务将扩大教育和培训计划，包括针对国防部人员和 DIB 承包商准备的材料，以提高他们的网络威胁意识。
  - 此外，国防情报助理部长办公室将审议当前有关关键收购和技术方案的分类指导在承包商网络信息保护方面的充分性。
- 加强国防部获取和采购的网络安全标准。为了保护国防部网络，国防部必须加强国防部获取和采购项目的网络安全要求，将网络安全标准纳入研究、开发和采购国工具的工作中。国防部将为业界指定其他网络安全标准，以满足任何国防部采购项目的组成部分要求。
- 在采购、情报、反间谍、执法和运营团队之间建立合作，以防止、减轻和响应数据丢失情况。国防部将建立一个联合采购保护与开发小组（JAPEC），来加强情报、反间谍和执法人员与采购项目管理人员之间的联系，防止和减少数据丢失和被盗情况。国防部将对网络间谍活动和窃取进行全面的风险和损失评估，以告知行动过程中的要求、采购、方案和反间谍活动。
  - 国防部首席信息官协同国防部采办、技术和物流助理部长办公室，将评估和更新具体信息系统的安全控制措施，在 NIST 和 DFARS 标准框架下为国防承包商巩固 DFAR。
  - 为了保障关键项目和技术安全性，国防部将与合作开发预警能力并建立分层的网络防御。
  - 最后，国防网络犯罪中心、国防部长首席网络顾问以及国防部采办、技术和物流助理部长办公室将与服务损害评估管理办公室加强合作，精简风险和损失评估流程，更好地就维持、修改或取消侵入程序做出决策。
- 使用反间谍国防部能力来防御网络入侵。军事部门和国防情报助理部长与首席网络顾问协商，将制定相关战略并经国防部长批准，以最大程度地提高军事部门的反间谍机构有关确认、追溯和防御网络入侵者的能力和权限。
  - 反间谍机关在提高我们挫败和战胜网络间谍活动能力方面有着得天独厚的优势。本战略将具体指出国防部反间谍机构如何更加有效地与美国广大情报和执法部门就调查、人力和技术行动加强协作，防止对手利用网络窃取美国及其盟友和合作

伙伴的知识产权。

- 支持政府的整体政策和能力来对抗知识产权窃取。国防部将继续与美国政府其他机构合作，应对通过网络空间所构成的知识产权盗窃的威胁。

### 实现目标 3

为保卫美国本土及关键利益做好准备，防御扰乱性或破坏性的网络攻击，避免造成严重后果。

- 继续开发情报和预警能力以预测潜在威胁。为了避免网络攻击给国家造成严重后果，国防部将与更多的情报机构开展合作，开发有关敌人活动的情报能力，并能够在网络攻击对美国本土和美国利益造成影响之前加以阻止。为了满足作战指挥应急要求，国防部将拓展有关主要敌人的人力和技术网络方面的情报。为保证网络空间有效地运作，国防部在未来行动的各个阶段都需要网络情报、预警和共享态势感知能力。所有的情报收集活动将遵循行政令列出的法律和指导规则。
- 开发和使用保卫国家的能力。国家任务部队和其他相关国防内设部门将与主要跨机构组织进行培训并建立伙伴关系，备战网络行动防止网络攻击给国家带来严重影响。此外，国防部将通过定期在各级部门实施应急演练规程，支持部门间演练紧急和蓄意的网络行动程序。
  - 建立伙伴关系，保卫国家安全。国防部将部署与其他政府机构的合作框架，开展保卫国家行动。国防部将与联邦调查局、中央情报局、国土安全部和其他机构建立合作关系并整合各方力量，为总统对严重网络攻击做出响应提供最多可选的方案。
  - 对国防部保卫国家的能力开展年度综合审查。随着时间的发展，国防部对防御严重网络攻击使命的要求和能力将会不断提升。国防部每年都将就这项任务已具备及所需的能力进行深入评估。作为评估的一部分，国防部将验证新出现的要求，找出差距和明确工作计划。
- 开发创新方法以保卫美国的关键基础设施。国防部将联合国土安全部改进网络安全增强服务计划，并鼓励更多的关键基础设施实体参与，特别是强调提高国防关键基础设施的参与者的数量。
- 开发自动化信息共享工具。为了提高共享态势感知，国防部将与国土安全部和其他机构共同与美国政府内部重要伙伴、关键盟国及合作军方、州与地方政府以及私营部门建立连续化、自动化、标准化的信息共享机制。此外，国防部将与其他美国政府机构和国会一起推动就美国政府和私营部门信息共享进行立法。
- 评估国防部的网络威慑态势与战略。建设国防科学委员会网络威慑工作组，美国战略司令部（USSTRATCOM）经与联合参谋部和国防部长办公室协调，将评估国防部防御特定的国家及非国家角色针对美国本土及美国利益发动重大网络攻击，攻击影响可能包括生命损失、重大破坏财产或者严重影响美国的外交和经济政策利益。
  - 美国战略司令部在分析过程中必须确定国防部是否能够对这类攻击中的主要威胁进行溯源和威慑，并针对国防部提高网络威慑态势的具体行动提出建议。应特别注意，尽管对非国家角色可能在传统威慑框架之外，但这类活动也可能给美国利益造成相当大的威胁。



#### 实现目标 4

建立并维护可行的网络空间方案,制定实施计划以控制冲突升级,在各个阶段改变冲突环境。

- 将网络方案纳入整体计划。为了满足武装力量招募指南、作战司令部计划及其他战略指导性文件定义的战略目标,国防部将与美国政府机构以及美国的盟友和伙伴加强合作,将网络方案加入到作战命令计划中。

- 加快把网络要求加入整体计划中。国防部将加快把网络要求整合到作战司令部计划中。这些计划必须概括和定义具体目标的网络空间影响。为了推动这项工作,联合参谋部将与美国战略司令部合作,将要求同步和整合到规划中,并向参谋长联席会议主席提供有关评价、分配、指派和任命网络任务部队的建议。

#### 实现目标 5

建立并维护强有力的国际联盟和合作伙伴关系,以防止共同风险,提高国际安全与稳定。

- 在重点区域建立合作伙伴能力。根据其当前和计划中的部队结构,国防部将与主要盟友和伙伴共同建立合作伙伴能力,并帮助保护国防部的任务和美国的利益所依赖的关键基础设施和关键资源。国防部将与美国政府其他机构包括国务院加强合作,建立合作伙伴能力。重点区域包括中东、亚太和欧洲。

- 支持中东地区盟友和伙伴提高网络及系统强度和韧性。作为其网络对话和伙伴关系的一部分,国防部将与主要的中东盟友和伙伴开展合作,以提高它们保护其军事网络以及美国利益所依赖的关键基础设施和关键资源的能力。主要举措包括提高信息共享,形成统一的网络威胁认知,评估共同的网络防御态势,以及合作的方式建立网络空间专业知识。

- 支持东北亚盟国网络及系统强度和韧性。作为更广泛的亚洲盟国网络对话的部分工作,国防部将与主要盟友和伙伴合作,以提高它们保护其军事网络以及美国利益所依赖的关键基础设施和关键资源的能力。

- 在亚太地区建立新的战略合作伙伴关系。国防部将按照符合美国国防部的《网络空间国际安全合作指南》的方式,与亚太地区联手建立网络能力,使美国利益和盟国的利益风险最小化。

- 与主要的北约盟国加强合作,以缓解美国国防部和美国国家利益的网络风险。国防部将通过国防部与主要的北约盟国开展的防务磋商来建立这类合作伙伴关系。

- 尽管建立了联盟和伙伴关系,国防部仍将保持自身灵活度和敏捷性,以对战略环境的变化做出最佳响应。

- 制定解决方案以应对破坏性恶意软件扩散。国家和非国家角色试图获取具有破坏性的恶意软件。如果让具有破坏性的恶意软件不受控制的扩散给敌方,将给国际体系带来严重隐患。与国务院、美国政府其他机构以及美国盟友和伙伴进行合作,国防部将参考最佳实践以应对具有破坏性的恶意软件在国际范围的扩散。除了国际制度和最佳实践,美国政府还有一系列国内出口管制制度,可用于防止军民两用技术的扩散。
- 与有能力的国际伙伴开展合作以规划和训练网络行动。为了贯彻这一战略的实施,国防部将加强其国际联盟和伙伴的合作,发展综合能力在网络效应上支持作战司令部计划。

- 加强中美网络对话，增强战略稳定性。在这一战略实施过程中，作为中美国防磋商会谈及相关对话的一部分，如网络工作组，国防部将继续保持与中国交流讨论，从而更好地了解各国在网络空间的军事理论、政策、角色和任务并提高透明度。这项工作的目的是为了降低误解和误判的风险，误解和误判可能导致矛盾升级和不稳定。国防部将支持美政府致力于加强建立信任措施，以将中美关系提升到更高水平。

## 5. 管理战略

为了实现本战略提出的目的和目标，要在网络力量、人员、组织和能力等方面做出谨慎选择。在实施这一战略过程中，国防部在财务方面的选择将影响全国甚至全球今后几年的发展，国防部必须以一种有效的和节约的方式运作，以确保其投资效益最优。为此，国防部将按照以下管理目标来管理其网络活动和任务：成立为国防部长服务的首席网络顾问办公室，提高网络预算管理，制定国防部网络运营和网络安全战略框架，针对国防部的网络战能力开展端到端评估等。

- 成立为国防部长服务的首席网络顾问办公室。在 2014 年的国防授权法（NDAA）中，国会要求国防部为国防部长指定首席网络顾问，负责审查涉及军事的网络空间活动、网络任务力量以及进攻性和防守性的网络行动和任务。此外，首席网络顾问将指导国防部网络空间政策和战略的发展。
  - 2014 年的国防授权法还规定，首席网络顾问综合网络专业知识和主要机构的观点来成立部门内核心团队，以确保在国防部内网络问题得到有效治理。2014 年国防授权法所指定的首席网络顾问的职责，不得被解释为影响国防部下述的职位的现有职责和权限，包括采办、技术和后勤助理部长，政策助理部长，情报助理部长，人事和战备助理部长以及任何其他国防部长办公室首席参谋助理（PSA）的网络相关职责与权限。
  - 成立跨部门团队。首席网络顾问将与网络投资和管理委员会（CIMB）的国防部代表共同对国防部的网络管理进行审查。网络投资和管理委员会将成为一个同步、协调和项目管理的平台。它既不会重复现有计划和预算机制，也不会影响先前确定的首席助理官的角色和权限，更不会以任何方式干预军事决策。相反地，它提供了一个整合网络计划的平台，将通过管理项目直至项目完成，并精简国防部的网络治理结构。该 PCA 将与国防部负责采办、技术和后勤的助理部长办公室和联合参谋部工作，以建立国防部代表组成的部门内的团队来支持网络投资和管理委员会的这项工作。
  - 高管论坛。隶属于网络投资和管理委员会并向其进行汇报，高管论坛将就关键网络问题进行初步的高层协调。该高管论坛将向网络投资和管理委员会提供行动建议，并协调其他 OSD 和联合参谋部治理机构，以促进工作的统一性并解决适当层次的管理问题。
  - 当预算或财务事项进入实施和预算审查过程时，首席网络顾问将利用高管论坛和 CIMB 来协调向代理管理行动小组或其他财务和预算组织提出建议，在处理问题过程中审批相关方案和替代方案。

- 提高网络预算管理。国防部将制定一种协商方法使国防部网络运营预算管理更加透明、更加有效。目前，网络方面的投入涉及国防部预算的方方面面，包括军事情报项目（MIP）、多项拨款、预算线、项目组成部分和项目本身。此外，由国防部情报助理部长代表国防部，确保所有国家情报项目（NIP）投资都用于支持国防部的任务。国防部网络预算的分散性质对国防部有效的预算管理来说是一个挑战，国防部必须制定用于跨项目资金管理的新方法，以提高任务有效性，实现高效管理。
- 制定国防部网络作战和网络安全政策框架。按照总统指示，国防部将调整和简化关于网络运营和网络安全策略管理，已发现的差距、重复、链接、冲突以及现有文档需要修订的部分。这项工作将有助于将国家和部门的指导和政策转化为战术行动。重要的是，要明晰在现有文档中使网络行动和网络安全管理复杂化的冲突之处。
- 针对国防部的网络战能力，开展端到端评估。美国网络司令部将对其态势进行综合作战评估。协调国防部长首席网络顾问，采办、技术和后勤助理部长办公室以及海岸评估和项目评价主管办公室，美国网络司令部（USCYBERCOM）将通过网络投资和管理委员会（CIMB）向国防部长提供短期和长期性的建议，主要涉及组织架构、指挥和命令机制以及有关参与、人员、能力、工具和潜在的运营差距等方面的规则。这种态势评估的目标是清楚地了解未来作战环境、关键利益相关者的意见以及规划和运行的战略重点、选择和资源。

## 6. 总结

我们生活在这样一个时代，针对美国利益的网络威胁不断增长。各种国家和非国家行为者针对美国颇具威胁性的破坏性、毁灭性的攻击，以及针对知识产权的网络窃密将削弱美国的科技和军事优势。我们的网络空间相当脆弱，当前网络威胁的规模之大，需要由跨越整个政府和私营部门的领导者和组织立即采取紧急行动。

自从 2011 年开发了第一版网络空间战略起，美国国防部已在建立网络战能力、发展组织和计划以及促进建立为保卫国家及其利益所必需的合作伙伴关系方面取得了显著的进展，但必须采取更多措施。从这一战略列出的目标可以引出，为确保取得进展，相关资源必须得到配置和管理。

这一战略提出了实现变革所需的积极、具体的计划。为了使国防部能够成功履行在网络空间捍卫美国及其利益的使命，来自整个政府部门的领导必须采取行动，以实现本战略中列出的目标。他们还必须履行其组织的职责。由于网络和计算机代码的自然特性，仅靠任何单独的组织难以完成这项工作。要取得成功，就需要整个国防部、美国政府机构、私营部门以及美国的盟友和伙伴之间的密切合作。

战略环境可能迅速变化，在网络空间尤为如此。在这项工作中，我们必须是动态、灵活和敏捷的。我们必须预见到新出现的威胁、识别出需要建设的新能力，并确定如何增强我们的合作伙伴关系和规划。与从前一样，我们的全体人员，无论是穿制服的人员还是文职人员，都将是我们最大、最持久的力量和灵感的根源。通过共同努力，我们将在这样一个数字化时代为保护和捍卫美国及其利益提供帮助。

---

## 二十八、2015 年网络安全法

奥巴马 2015 年 12 月签字实施

---

## 第 1 条 简称及目录

### (a) 简称

本法可被称为“2015 年网络安全法”。

### (b) 目录

本法目录如下所示：

#### 第 1 条 简称及目录

#### 第 I 章 网络安全信息共享（第 101～111 条）

##### 第 101 条 简称

##### 第 102 条 定义

##### 第 103 条 联邦政府信息共享

##### 第 104 条 对预防、检测、分析和减轻网络安全威胁的授权

##### 第 105 条 与联邦政府共享网络威胁迹象信息和防护措施

##### 第 106 条 免责

##### 第 107 条 对政府活动的监督

##### 第 108 条 解释和优先

##### 第 109 条 网络安全威胁报告

##### 第 110 条 国防部部长传播特定信息的权限所受限制的例外情况

##### 第 111 条 生效期限

#### 第 II 章 国家网络安全增强（第 201～229 条）

#### 第 A 节 国家网络安全和通信整合中心（第 201～211 条）

##### 第 201 条 简称

##### 第 202 条 定义

##### 第 203 条 信息共享框架和流程

##### 第 204 条 信息共享和分析组织

##### 第 205 条 国家响应框架

##### 第 206 条 降低国土安全部数据中心网络安全风险的报告

##### 第 207 条 评估

##### 第 208 条 关键基础设施中多个并发的网络事件

##### 第 209 条 美国口岸网络安全脆弱性报告

##### 第 210 条 新监管权限的禁止事项

##### 第 211 条 提交报告要求的期限

#### 第 B 节 联邦网络安全增强（第 221～229 条）

##### 第 221 条 简称

##### 第 222 条 定义

##### 第 223 条 联邦网络安全的增强

##### 第 224 条 高级内部防御

第 225 条 联邦网络安全要求

第 226 条 评估和报告

第 227 条 终止

第 228 条 国家安全相关信息系统的识别

第 229 条 机构指引

### 第III章 联邦网络安全人员评价（第 301～305 条）

第 301 条 简称

第 302 条 定义

第 303 条 国家网络安全人员评价计划

第 304 条 具有关键需求的网络相关工作角色的确定

第 305 条 政府问责办公室进展报告

### 第IV章 其他网络事项

第 401 条 移动设备安全研究

第 402 条 国务院国际网络空间政策战略

第 403 条 国际网络犯罪分子的逮捕与起诉

第 404 条 应急服务增强

第 405 条 提高医疗卫生行业的网络安全

第 406 条 联邦计算机安全

第 407 条 禁止对美国人民金融信息进行欺诈性销售

## 第 I 章 网络安全信息共享（第 101 ~ 111 条）

### 第 101 条 简称

本章可被称为“2015 年网络安全信息共享法”。

### 第 102 条 定义

在本章中：

（1）机构——是指《美国法典》第 44 编第 3502 条所定义的机构。

（2）反垄断法——是指：

（A）《克莱顿法》第 1 条（《美国法典》第 15 编第 12 条）所定义的反垄断法；

（B）包括《联邦贸易委员会法》第 5 条（《美国法典》第 15 编第 45 条）在内，并扩展该条以适用于不正当竞争的情况；

（C）包括各州反垄断法中与上述（A）、（B）相一致的内容。

（3）有关联邦实体——是指：

（A）商务部；

（B）国防部；

（C）能源部；

（D）国土安全部；

（E）司法部；

(F) 财政部;

(G) 国家情报总监办公室。

(4) 网络安全目的——是指保护信息系统或系统中存储、处理或传输的信息,免受网络安全威胁或安全脆弱性的影响。

(5) 网络安全威胁

(A) 一般规定——是指在信息系统上或通过信息系统实施的、可能对信息系统或系统中存储、处理或传输的信息的安全性、可用性、保密性、完整性造成不利影响的未授权行为。此类行为不受《美国宪法》第一修正案保护,(B)中另有规定的除外。

(B) 例外情况——不包括仅涉及违反消费服务条款或消费者许可协议的行为。

(6) 网络威胁迹象信息——是指描述或识别以下情况所需的必要信息:

(A) 恶意侦查,包括为收集网络安全威胁或安全脆弱性相关技术信息而发送的异常通信;

(B) 使安全控制失效或利用安全脆弱性的方法;

(C) 安全脆弱性,包括可能表明存在安全脆弱性的异常活动;

(D) 造成合法用户在合法访问信息系统或系统中存储、处理或传输的信息的情况下,无意关闭安全控制或使安全脆弱性可被利用的方法;

(E) 恶意网络指令和控制;

(F) 安全事件造成的实际或潜在危害,如某些网络安全威胁导致的信息泄露;

(G) 法律允许发布的网络安全威胁的其他属性;

(H) 上述情况的任意组合。

(7) 防护措施

(A) 一般规定——是指为检测、阻止或减轻已知的或疑似的网络安全威胁或安全脆弱性,应用于信息系统或系统中存储、处理或传输的信息的行为、设备、程序、签名、技术或其他措施,(B)目中另有规定的除外。

(B)例外情况——不包括会造成下述实体以外的其他实体拥有的信息系统或系统信息遭受破坏、不可用、未授权访问或极大损害的措施:

(i) 运行防护措施的私营实体;

(ii) 已经允许或授权允许私营实体运行防护措施的其他实体或联邦实体。

(8) 联邦实体——是指美联邦部、局或其组成部分。

(9) 信息系统——是指:

(A) 《美国法典》第 44 编第 3502 条所定义的信息系统;

(B) 包括工业控制系统,如监控和数据收集系统、分布式控制系统、可编程逻辑控制器等。

(10) 地方政府——是指各州的任何自治市、市、郡、教区、镇、镇区、乡村或其他政区政府。

(11) 恶意网络指令和控制——是指未经授权而远程识别、访问、使用信息系统或系统中存储、处理或传输信息的方式。

(12) 恶意侦查——是指与已知或疑似的网络安全威胁有关、以发现信息系统安全脆弱性为目的主动探测或被动监测信息系统的方法。

(13) 监控——是指获取、识别、扫描或占有信息系统中存储、处理或传输的信息。

(14) 非联邦实体

(A) 一般规定——是指私营实体、非联邦的政府机构或部门，以及各洲、部落或地方政府（包括其下设机构、部门及组成部分）。本款中另有规定的除外。

(B) 包含事项——包括哥伦比亚特区、波多黎各自由联邦、美属维尔京群岛、关岛、美属萨摩亚、北马里亚纳群岛以及其他美国领土或领地的政府机构或部门。

(C) 例外情况——不包括《1978 年外国情报监听法》第 101 条（《美国法典》第 50 编第 1801 条）所定义的外国势力。

(15) 私营实体

(A) 一般规定——是指个人或私营团体、组织、独资企业、合资企业、信托、合作企业、公司，或其他商业性质或非营利性质的实体，包括其管理人员、员工或代理人。

(B) 包含事项——包括提供公共服务（如电力、天然气、水等）的州、部落或地方政府。

(C) 例外情况——不包括《1978 年外国情报监听法》第 101 条（《美国法典》第 50 编第 1801 条）所定义的外国势力。

(16) 安全控制——是指用以保护信息系统或系统信息的保密性、完整性和可用性，免受非授权行为造成不利影响的管理、操作和技术等控制措施。

(17) 安全脆弱性——是指任何可能造成或促使安全控制失效的硬件、软件、进程和程序的属性。

(18) 部落——是指《印第安民族自决与教育援助法案》第 4 条（《美国法典》第 25 编第 450b 条）所定义的印第安部落。

### 第 103 条 联邦政府信息共享

(a) 一般规定

国家情报总监、国土安全部部长、国防部部长以及司法部长，应会同有关联邦实体负责人，综合考虑对涉密信息、情报来源和获取方法以及公民隐私和自由的保护，制定并颁布相关程序以促进和推动以下事项：

(1) 及时同经过安全审查的相关联邦实体、非联邦实体代表共享联邦政府掌握的涉密网络威胁迹象信息和防护措施。

(2) 及时与相关联邦实体、非联邦实体，共享联邦政府掌握的、可适当解密至非涉密级的网络威胁迹象信息、防护措施以及与网络安全威胁相关的信息或本章中授权使用的信息。

(3) 及时与相关联邦实体、非联邦实体或适当范围的公众共享联邦政府掌握的非涉密（包括受控非涉密）网络威胁迹象信息和防护措施。

(4) 适当情况下，及时与联邦实体、非联邦实体，共享联邦政府拥有的、与这些实体有关的网络安全威胁信息，以防止或减轻威胁带来的不利影响。

(5) 关注小型企业（定义参见小型企业法第 3 条（《美国法典》第 15 编第 632 条））面临的访问性与实施方面的问题，持续分析网络威胁迹象信息、防护措施、网络安全威胁以及对本章授权使用的有关信息，形成网络安全最佳实践，并通过出版物和针对性的推广活动与中小型企业共享。

(b) 制定有关程序



(1) 一般规定——根据本条 (a) 款制定的程序，应满足以下要求：

(A) 在保障涉密信息安全的情况下，确保联邦政府具备（且能够持续具备）实时共享网络威胁迹象信息和防护措施的能力。

(B) 为推进联邦政府共享信息，应最大程度地整合联邦实体和非联邦实体已有的流程、角色和职责，包括各关键基础设施具体行业的信息共享和分析中心。

(C) 制定相应程序，对根据本章规定接收联邦政府分享的网络威胁迹象信息或防护措施的联邦实体和非联邦实体，一旦发现或可以确定该实体出现错误或违反了本章规定以及联邦其他法律法规的规定，应及时通知。

(D) 对共享网络威胁迹象信息或防护措施的联邦实体提出要求应实施或应用安全控制，以保护上述网络威胁迹象信息或防护措施避免未经授权访问或获取。

(E) 包括相应程序，要求联邦实体在共享网络威胁迹象信息之前：

(i) 审查该网络威胁迹象信息，评估其中是否含有与网络安全威胁无直接关系的、共享时该联邦实体已知晓是具体人员个人信息，或能够用于识别具体人员的信息，如果是，应予以删除；

(ii) 或使用技术手段直接删除与网络安全威胁无直接关系的、共享时该联邦实体已知晓是具体人员个人信息或能够用于识别具体人员的信息。

(F) 并且包括相应程序，一旦发现或可以确定有联邦实体违反本款规定共享了任何美国公民的个人信息，应及时通知该公民。

(2) 协商——在制定本条所述流程时，国家情报总监、国土安全部部长、国防部部长及司法部长应与有关联邦实体协商，包括小企业管理局和国家实验室（定义参见 2005 年《能源政策法》第 2 条（《美国法典》第 42 编第 15801 条））等，以确保制定的流程能够有效促进和推动联邦政府对网络威胁迹象信息的及时共享。

(c) 向国会提交

本法颁布之日起 60 日内，国家情报总监应与有关联邦实体负责人协商，将根据本条 (a) 款制定的程序提交至国会。

## 第 104 条 对预防、检测、分析和减轻网络安全威胁的授权

(a) 对监控的授权

(1) 一般规定——尽管其他法律可能另有规定，为了保护网络安全，私营实体可监控：

(A) 本私营实体的信息系统；

(B) 其他非联邦实体的信息系统，但须获得该非联邦实体的授权和书面许可；

(C) 联邦实体的信息系统，但须获得该联邦实体授权代表的授权和书面许可；

(D) 本款允许私营实体监控的信息系统中存储、处理或者传输的信息。

(2) 说明——本条中的任何规定不应被解释为：

(A) 除按照本章规定之外，授权监控某个信息系统，或使用通过违规监控获取的任何信息；

(B) 限制其他合法活动。

(b) 对实施防护措施的授权

(1) 一般规定——尽管其他法律可能另有规定，为了保护网络安全，私营实体可在下述信

息系统中实施防护措施：

(A) 本私营实体的信息系统，以保护自身权利或财产；

(B) 其他非联邦实体的信息系统，以保护该非联邦实体权利或财产，但需获得该非联邦实体对执行这些防护措施的书面许可；

(C) 联邦实体的信息系统，以保护该联邦实体权利或财产，但需获得该联邦实体授权代表对执行这些防护措施的书面许可。

(2) 说明——本条中的任何规定不应被解释为：

(A) 除本条允许的范围之外，授权使用防护措施；

(B) 限制其他合法活动。

(c) 对共享或接收网络威胁迹象信息或防护措施的授权

(1) 一般规定——尽管其他法律可能另有规定，为了保护网络安全和涉密信息，非联邦实体可以共享或接收其他非联邦实体或联邦政府的网络威胁迹象信息或防护措施，(2) 项中另有规定的除外。

(2) 法律限制——在接收其他联邦实体或非联邦实体的网络威胁迹象信息或防护措施时，非联邦实体应遵守这些实体对共享或使用此类网络威胁迹象信息或防护措施做出的法律限制。

(3) 说明——本条中的任何规定不应被解释为：

(A) 除按照本条规定之外，授权共享或接收网络威胁迹象信息或防护措施；

(B) 限制其他合法活动。

(d) 信息的保护和使用

(1) 信息的安全——根据本条规定，在监控信息系统、实施防护措施、提供或接收网络威胁迹象信息和防护措施时，非联邦实体应实施和应用安全控制，以保护上述网络威胁迹象信息或防护措施免受未经授权访问或获取。

(2) 个人信息的删除——根据本章规定共享网络威胁迹象信息前，非联邦实体应：

(A) 审查该共享的网络威胁迹象信息，评估其中是否含有与网络安全威胁无直接关系的、共享时该非联邦实体已知晓是具体人员个人信息，或能够用于识别具体人员的信息，如果是，应予以删除。

(B) 或使用技术手段直接删除与网络安全威胁无直接关系的、共享时，该非联邦实体已知晓是具体人员个人信息或能够用于识别具体人员的信息。

(3) 非联邦实体对网络威胁迹象信息和防护措施的使用。

(A) 一般规定——在遵守本章规定的前提下，为了保护网络安全，根据本章规定共享或接收的网络威胁迹象信息或防护措施，可以：

(i) 被非联邦实体用于监控以下信息系统或对其实施防护措施：

(I) 该非联邦实体的信息系统；

(II) 其他联邦实体或非联邦实体的信息系统，但需获得对方的书面许可。

(ii) 被非联邦实体在其他方面使用、保留或进一步共享，但需遵守以下规定：

(I) 共享该网络威胁迹象信息或防护措施的联邦实体或非联邦实体对其做出的法律限制；

(II) 其他适用的法律规定。

(B) 说明——本款中的任何规定不应被解释为，授权使用本条规定之外的网络威胁迹

象信息或防护措施。

(4) 州、部落或地方政府对网络威胁迹象信息的使用。

(A) 用于执法——出于本法第 105 条第 (d) 款第 (5) 项第 (A) 目部分描述的目的，州、部落或地方政府可使用根据本法规定接收的网络威胁迹象信息或防护措施。

(B) 披露免责——根据本条规定，在州、部落或地方政府（或州、部落、地方政府组建的私营实体）间共享的网络威胁迹象信息或防护措施，应：

(i) 被视为自愿共享的信息；

(ii) 并且根据州、部落或地方信息自由法、公开政府法、公开会议法、公开记录法、阳光法或其他类似对披露信息或记录有要求的法律进行披露，不用承担法律责任。

(C) 州、部落及地方监管部门。

(i) 一般规定——州、部落或地方政府依本法共享的网络威胁迹象信息或防护措施，不得被州、部落或地方政府用于监管（包括采取执法行动）任何非联邦实体的合法活动，或非联邦实体根据强制性标准开展的活动，包括与监控、实施防护措施或共享网络威胁迹象信息有关的活动，第 (ii) 段中另有规定的除外。

(ii) 与预防或减轻网络安全威胁有关的监管授权——在符合州、部落或地方政府监管权限（尤其是与预防或减轻信息系统的网络安全威胁相关的权限）的前提下，根据第 (i) 段中规定共享的网络威胁迹象信息或防护措施，可用于开展或实施对于此类信息系统的监管。

(e) 反垄断豁免

(1) 一般规定——在本法框架下，为了保护网络安全，两家或两家以上私营实体交换或相互提供网络威胁迹象信息、防护措施，或协助用于预防、调查或减轻网络安全威胁的行为，不违反反垄断法，第 108 条第 (e) 款中另有规定的除外。

(2) 适用性——第 (1) 项仅适用于为协助以下情况而交换的信息或提供的协助：

(A) 有助于预防、调查或减轻信息系统或系统中存储、处理或传输的信息面临的网络安全威胁。

(B) 沟通或披露网络威胁迹象信息，以帮助预防、调查或减轻网络安全威胁对信息系统或系统中存储、处理或传输的信息造成的不利影响。

(f) 无权利或利益

根据本章规定，与非联邦实体共享网络威胁迹象信息或防护措施，不应为该非联邦实体或其他任何非联邦实体的类似信息产生任何权利或利益。

## 第 105 条 与联邦政府共享网络威胁迹象信息和防护措施

(a) 政策和程序要求

(1) 过渡政策和程序——本法颁布之日起 60 日内，司法部长、国土安全部长应会同有关联邦实体的负责人，制定相关联邦政府接收网络威胁迹象信息和防护措施的过渡政策和程序，并提交至国会。

(2) 最终政策和程序——本法颁布之日起 180 日内，司法部长、国土安全部长应会同有关联邦实体的负责人，制定并颁布有关联邦政府接收网络威胁迹象信息和防护措施的最终政策和程序。

(3) 政策和程序相关要求——根据本条制定或颁布的政策和程序，应符合本条 (b) 款规定的要求，并应：

(A) 确保非联邦实体根据第 104 条 (c) 款的规定，利用本条第 (c) 款所述实时流程，与联邦政府共享的网络威胁迹象信息符合以下规定：

(i) 自动与所有有关联邦实体共享；

(ii) 只能根据实时流程中已规定的措施而进行延迟、修改或被采取其他行为，这会影响所有有关联邦实体对信息的实时接收，故只能当这种延迟、修改或其他行为满足以下条件时进行：

(I) 经所有有关联邦实体的负责人一致同意。

(II) 在联邦实体保留或使用网络威胁迹象信息或防护措施之前实施。

(III) 是统一应用的，每个有关联邦实体都可能受到同样的延迟、修改或其他行为的影响。

(iii) 可提供给其他联邦实体。

(B) 确保非联邦实体根据第 104 条的规定，以本条第 (c) 款所述实时流程以外的方式与联邦政府共享的网络威胁迹象信息：

(i) 在可行的情况下，尽快与所有有关联邦实体共享。

(ii) 不受到任何不必要的延期、干扰或其他行为的影响，以免影响所有有关联邦实体的接收。

(iii) 并且可提供给其他联邦实体。

(C) 确保具有：

(i) 审计机制；

(ii) 设置了相应的惩罚措施，防止联邦实体的官员、雇员或代表联邦政府的机构，在本章下以非授权的方式明知故犯。

(4) 实体与联邦政府共享网络威胁迹象信息的指南。

(A) 一般规定——本法颁布之日起 60 日内，司法部长和国土安全部长应联合制定并发布可行的指导文件，以协助和促进各实体根据本章规定与联邦实体共享网络威胁迹象信息。

(B) 内容——根据 (A) 目中制定并发布的指导文件，应包括以下内容：

(i) 确定哪些类型信息可作为符合本章要求的网络威胁迹象信息，其中不应包含如下信息：

(I) 与网络安全威胁无直接关联的信息；

(II) 具体人员的个人信息或可用于识别具体人员的信息。

(ii) 确定哪些类型信息受其他隐私法律法规保护且与网络安全威胁没有直接关系。

(iii) 根据本章规定，司法部长和国土安全部长认为适用于实体与联邦实体共享网络威胁迹象信息的其他事项。

(b) 隐私和公民自由

(1) 过渡指南——本法颁布之日起 60 日内，司法部长和国土安全部部长，应与有关联邦实体的负责人，以及根据《2004 年国家情报改革法》第 1062 条（《美国法典》第 42 编第 2000ee - 1 条）规定指定的官员协商，联合制定并公布关于隐私和公民自由保护的过渡指南，管理联邦实体通过本章授权活动获得的网络威胁迹象信息的接收、留存、使用或传播等行为，

并提交至国会。

(2) 最终指南。

(A) 一般规定——本法颁布之日起 180 日内，司法部长和国土安全部部长应与有关联邦实体的负责人、根据《2004 年国家情报改革法》第 1062 条（《美国法典》第 42 编第 2000ee - 1 条）规定指定的官员，以及司法部长和国土安全部部长认为相关领域具有丰富专业经验的私营实体协商，联合签发和公布关于隐私和公民自由保护的最终指南，管理联邦实体通过本章授权活动获得的网络威胁迹象信息的接收、留存、使用或传播等行为。

(B) 定期审查——司法部长和国土安全部部长应会同有关联邦实体的负责人、(A) 目所述官员及私营实体定期（每 2 年不少于 1 次）联合审查根据 (A) 目规定发布的指南。

(3) 内容——根据第 (1)、(2) 项要求制定的指南，应满足保护信息系统免受或减轻网络安全威胁的需求，同时应：

(A) 限制联邦政府根据本章规定采取的活动对隐私和公民自由的影响。

(B) 通过以下方式，限制包含具体人员个人信息或可用于识别具体人员的信息的网络威胁迹象信息的接收、留存、使用及传播：

(i) 制定有关流程，及时销毁已知与本章授权使用无直接关系的信息。

(ii) 制定限定要求，规定留存网络威胁迹象信息的专门期限。

(C) 提出相应要求，保护含有具体人员个人信息或可用于识别具体人员的信息的网络威胁迹象信息免受未经授权访问或获取，以及对联邦实体官员、雇员或代理机构违反本指南行为的适当制裁措施。

(D) 根据本章规定、任何其他可适用的法律条款，以及总统于 2011 年 4 月发布的《国家网络空间可信身份战略》附录 A 中所述公平信息实践原则，对联邦政府共享的网络威胁迹象信息的留存、使用或传播进行监管，如果可能，要监管联邦政府对这些网络威胁迹象信息的使用范围。

(E) 提出相应的通知程序，如果根据本条要求接收到信息后，接收信息的联邦实体知道或认定此信息不算威胁迹象信息，则要通知各实体和联邦实体。

(F) 对含有具体人员的个人信息或可用于识别具体人员的信息的网络威胁迹象信息，应在切实可行的情况下最大程度地保护其保密性，并要求告知接收方，该网络威胁迹象信息仅可在本章授权允许的情况下使用。

(G) 包括必要的措施，确保网络威胁迹象信息的传播符合涉密信息及其他敏感的国家安全信息保护的要求。

(c) 国土安全部内部职能和流程

(1) 一般规定——本法颁布之日起 60 日内，国土安全部部长应与有关联邦实体的负责人协商，制定并执行国土安全部内部职能和流程，以满足以下要求：

(A) 根据本条规定，实时接收来自任何非联邦实体的网络威胁迹象信息和防护措施。

(B) 根据本款第 (2) 项规定，能够证明国土安全部内部职能和流程可按照第 (2) 项要求全面、有效地运行后，将此作为联邦政府的信息接收流程明确下来，以通过电子邮件或媒体、互联网站上的互动表格，或信息系统间实时自动程序等方式，接收非联邦实体共享的网络威胁迹象信息和防护措施。下述通信除外：

(i) 根据第 104 条规定，联邦实体与非联邦实体之间的通信，主要基于以前已经共享的信息，用于描述相关网络安全威胁或开发相应防护措施。

(ii) 受监管的非联邦实体与监管该实体的联邦监管部门之间，就网络安全威胁进行的通信。

(C) 确保所有有关联邦实体，能够通过国土安全部内部实时程序，自动接收共享的网络威胁迹象信息和防护措施。

(D) 与本条规定中要求的政策、章程和指南相一致。

(E) 不限制或禁止通信、记录或其他信息的合法披露，包括：

(i) 非联邦实体向其他非联邦实体或联邦实体报告已知或疑似的犯罪活动，包括为促进启动联邦执法调查而与联邦实体共享的网络威胁迹象信息或防护措施；

(ii) 自愿或依法律强制要求参与联邦调查；

(iii) 根据法定或授权合同要求，提供网络威胁迹象信息或防护措施。

(2) 证明和指定。

(A) 职能和流程的证明——本法颁布之日起 90 日内，国土安全部长应与有关联邦实体的负责人协商，向国会提交一份证明，描述第 (1) 项规定的职能和流程是否按如下方式完全、有效地实施：

(i) 该流程可以供联邦政府从任何非联邦实体处接收网络威胁迹象信息或防护措施。

(ii) 符合本章规定的过渡政策、程序和指南。

(B) 指定。

(i) 一般规定——总统可在 (A) 目所述证明提交后的任何时间，指定一个合适的联邦实体[国防部（包括国家安全局）除外]，制定并实施国土安全部部长未能覆盖的职能和流程。前提是做出这一指定前不少于 30 日，总统就已经向国会提交相关证明和解释材料，阐明以下事项：

(I) 上述指定是必需的，以确保根据本章规定，联邦政府可从任何非联邦实体处接收网络威胁迹象信息或防护措施的职能和流程能够完全、有效和稳定地执行。

(II) 被指定的合适联邦实体，能够按本章规定（包括第 (a) 款第 (3) 项第 (A) 目）制定的政策、程序和指南要求，接收和共享网络威胁迹象信息和防护措施。

(III) 并且上述指定与该联邦实体的使命是一致的，并能够增强联邦政府接收、共享和使用本章授权的网络威胁迹象信息和防护措施的能力。

(ii) 对其他职能和流程的适用性——如果总统根据第 (i) 段要求指定了合适联邦实体制定并实施相关职能和流程，本章中适用于第 (1) 项要求的职能和机制的规定，将被理解为也适用于根据第 (i) 段要求制定并实施的职能和流程。

(3) 公告与访问——国土安全部部长应确保根据第 (1) 项要求制定和实施的职能与流程能够广而告之，并易于访问，以使：

(A) 任何非联邦实体，均可通过该流程与联邦政府共享网络威胁迹象信息和防护措施。

(B) 所有有关联邦实体，均可利用国土安全部根据本条 (a) 条制定的政策和程序来实时接收网络威胁迹象信息和防护措施。

(4) 其他联邦实体——根据第 (1) 项制定和实施的流程，应确保其他联邦实体能够通过该流程及时接收到与联邦政府共享的任何网络威胁迹象信息和防护措施。

(d) 与联邦政府共享或向其提供的信息

(1) 不放弃权限或保护——根据本章规定，向联邦政府提供网络威胁迹象信息和防护措施的规定，不应导致放弃任何相关法定的权限或保护，包括商业秘密的保护。

(2) 专属信息——根据第 104 条 (c) 款 (2) 项及其他任何可适用的法律条款规定, 非联邦实体根据本章要求向联邦政府提供网络威胁迹象信息或防护措施时, 如果发送信息的非联邦实体或持有书面授权代理第三方实体声明了这是其商业、金融和专属信息, 则该信息就应被作为商业、金融和专属信息对待。

(3) 披露免责——根据本章规定, 与联邦政府共享的网络威胁迹象信息和防护措施, 应:

(A) 被视为自愿共享信息, 免于《美国法典》第 5 编第 552 条所要求的披露, 免于各州、部落或地方的法律规定对信息或记录所要求的披露。

(B) 只要表示拒绝, 可免于《美国法典》第 5 编第 552 条 (b) 款 (3) 项 (B) 目所要求的公开, 免于各州、部落或地方的法律规定对信息或记录所要求的公开。

(4) 单向联系——本章向联邦政府提供网络威胁迹象信息或防护措施的条款, 不受任何联邦部、局或司法原则中有关与决策官员单向联系的限制。

(5) 披露、留存与使用。

(A) 授权的活动——根据本章要求向联邦政府提供的网络威胁迹象信息与防护措施, 在符合其他可适用的联邦法律规定情况下, 在披露给联邦部、局或其机构、官员、雇员、代理人, 或由其留存和使用时, 仅用于:

(i) 保护网络安全;

(ii) 确定:

(I) 网络安全威胁和其来源;

(II) 安全脆弱性。

(iii) 响应、避免或减轻特定的、会造成死亡、严重人身伤害或严重经济损失的威胁, 包括恐怖行动或大规模杀伤性武器的使用。

(iv) 响应、调查、起诉, 或避免、减轻对未成年人的严重威胁, 包括性剥削、对人身安全的威胁等。

(v) 预防、调查、阻止或起诉第 (iii) 段所述威胁造成的, 或下述法律条款规定的任何犯罪行为:

(I) 《美国法典》第 18 编第 1028~1030 条 (有关诈骗和身份盗用);

(II) 《美国法典》第 18 编第 37 章 (有关间谍活动及审查);

(III) 《美国法典》第 18 编第 90 章 (有关商业秘密的保护)。

(B) 禁止的活动——根据本章规定向联邦政府提供的网络威胁迹象信息及防护措施, 不得在 (A) 目允许的使用范围外, 披露给任何的联邦部、局或由其留存、使用。

(C) 隐私和公民自由——根据本章规定向联邦政府提供的网络威胁迹象信息及防护措施, 应由联邦政府按以下方式留存、使用和传播:

(i) 符合根据第 (a)、(b) 款规定制定的政策、程序和指南。

(ii) 防止未授权使用或披露含有以下信息的网络安全威胁迹象信息:

(I) 具体人员的个人信息;

(II) 能够识别具体人员身份的信息。

(iii) 能够保护含有以下信息的网络威胁迹象信息的保密性:

(I) 具体人员的个人信息;

(II) 能够识别具体人员身份的信息。

(D) 联邦监管部门。

(i) 一般规定——根据本章规定向联邦政府提供的网络威胁迹象信息及防护措施，不得被任何联邦、各州、部落或地方政府用于监管（包括执法行动）任何非联邦实体的合法活动，及其根据强制性标准要求开展的活动，包括与监控、实施防护措施或共享网络威胁迹象信息相关的活动，第（ii）段中另有规定的除外。

(ii) 例外情况：

(I) 负责预防或减轻网络安全威胁的监管部门。根据本章规定向联邦政府提供的网络威胁迹象信息和防护措施，可按照联邦或各州负责预防或减轻信息系统网络安全威胁的监管部门要求，通报该信息系统相关管理规定的制定或实施情况。

(II) 依据本章制定、实施的程序；第（i）段不适用于根据本章规定而制定并实施的程序。

## 第 106 条 免责

(a) 信息系统的监控

在符合本章规定的情况下，私营实体对第 104 条（a）款所述信息系统或信息实施监控活动，不应受到任何法院的起诉；对已提起诉讼的，法院应立即驳回。

(b) 网络威胁迹象信息的共享或接收

在下述情况下，私营实体根据第 104 条（c）款共享或接收网络威胁迹象信息或防护措施的行为，不应受到任何法院的起诉；对已提起诉讼的，法院应立即驳回：

(1) 私营实体的共享或接收行为符合本章规定；

(2) 网络威胁迹象信息或防护措施的接收方是联邦政府，共享方式符合第 105 条（c）（1）

(B) 目规定，并且共享或接收行为（视具体情况而定）开始于以下较早日期之后：

(A) 将第 105 条（a）（1）项要求的过渡政策和程序、第 105 条（b）（1）项要求的指南提交至国会的日期；

(B) 或本法颁布后第 60 天。

(c) 说明

本章中的任何规定不应被解释为：

(1) 产生以下责任：

(A) 共享网络威胁迹象信息或防护措施；

(B) 或基于接收的网络威胁迹象信息或防护措施，发出警告或采取行动。

(2) 或削弱或限制根据其他适用的不成文法或成文法进行抗辩的有效性。

## 第 107 条 对政府活动的监督

(a) 实施情况报告

(1) 一般规定——本法颁布之日起 1 年内，有关联邦实体的负责人应联合向国会提交一份详细报告，说明对本章的实施情况。

(2) 内容——上述（1）项要求的报告应包括相关联邦实体的负责人提出的建议，并描述如何改进或修改本章所述权限、政策、程序和指南，以及下列内容：

(A) 在实施第 105 条（c）款所述职能和流程时，对实时信息共享的有效性和障碍所进行的评估。

(B) 对网络威胁迹象信息或防护措施是否进行了正确标密进行评价，还要评估，出于



与私营部门共享网络威胁迹象信息或防护措施的目的，联邦政府是否对授权发放的安全许可证的次数有审计措施。

(C) 通过第 105 条 (c) 款所述职能和流程，接收网络威胁迹象信息或防护措施的数量。

(D) 根据本章规定，接收了网络威胁迹象信息或防护措施的联邦实体清单。

(b) 对合规性的双年度报告

(1) 一般规定——本法颁布之日起 2 年内，且此后每 2 年至少 1 次，各相关联邦实体的检查长应与情报共同体检查长、财政监督检查长委员会相协商，联合向国会提交一份跨机构报告，说明近两年来，联邦政府行政部门为落实本法规定所采取的行动。

(2) 内容——第 (1) 项所述双年度报告，应包括其涵盖时间范围内的以下事项：

(A) 评价用于联邦政府内部共享网络威胁迹象信息的政策、程序和指南的充分性，包括用于删除与网络安全威胁无直接关系信息（即具体人员的个人信息和可识别具体人员身份的信息）的相关政策、程序和指南。

(B) 评价网络威胁迹象信息或防护措施是否进行了正确标密，并审计为与私营部门共享网络威胁迹象信息或防护措施，联邦政府授权发放的安全许可证的次数。

(C) 对联邦政府根据本章规定接收到共享的网络威胁迹象信息或防护措施后，开展了哪些行动进行总结，总结报告包括以下内容：

(i) 联邦政府接收到网络威胁迹象信息或防护措施后，是否进行了正确使用和传播。

(ii) 网络威胁迹象信息或防护措施是否通过及时、适当的方式与有关联邦实体进行了共享，或（在适当的情况下）向社会公布。

(D) 对根据本章要求与有关联邦实体所共享的网络威胁迹象信息或防护措施进行评估，包括：

(i) 通过第 105 条 (c) 款要求所制定的职能和流程，共享的网络威胁迹象信息或防护措施的数量。

(ii) 与网络安全威胁无直接关系的任何信息（即具体人员个人信息和可识别具体人员身份的信息）的评估，包括非联邦政府实体违反本章规定与联邦政府共享的信息，或联邦政府违反本章所要求制定的指南，在其内部共享的信息以及对严重违反本章规定行为的说明。

(iii) 根据司法部长的统计，为了起诉第 105 条 (d) (5) (A) 目所述违法行为，联邦实体使用依据本章共享的信息的次数。

(iv) 针对具体人员个人隐私和公民自由保护，定性、定量地评价由于与联邦政府共享网络威胁迹象信息或防护措施而带来的影响，具体人员包括在未删除与网络安全威胁无直接关系的信息（即具体人员个人信息及可识别具体人员身份的信息）的情况下，根据第 105 条 (b) (3) (E) 目规定程序发布通知的次数。

(v) 联邦政府为减轻在开展本章要求的活动时对美国民众个人隐私和公民自由造成的不利影响，而采取措施的充分性。

(E) 评价邦实体间共享网络威胁迹象信息或防护措施的情况，识别出影响共享的不利因素。

(3) 建议——本款要求提交的报告可以包括由检查长提出的、用于改进或修改本章所述权限和流程的建议。

(c) 删除个人信息的独立报告

本法颁布之日起 3 年内，美国总审计长应向国会提交一份报告，说明根据本章规定，为删除网络威胁迹象信息或防护措施中包含的个人信息，联邦政府采取的各项行动。该报告还应评估，在解决个人隐私和公民自由保护问题方面，本章要求的政策、程序和指南是否充分。

(d) 报告的形式

本条要求的所有报告，均应以非涉密的形式提交，但可包含涉密附件。

(e) 报告的公开

本条要求的所有报告中，非涉密内容应向社会公开。

## 第 108 条 解释和优先

(a) 其他合法披露

本章中的任何规定不应被解释为：

(1) 限制或禁止非联邦实体，向本章所述任何其他非联邦实体或联邦政府，合法披露通信、记录或其他信息，包括报告已知或疑似的犯罪活动。

(2) 或限制或禁止任何联邦实体对上述披露信息的其他合法使用，包括对本章所要求的披露内容进行复制或再次披露。

(b) 举报者的保护

本章中的任何规定不应被解释为，禁止或限制受以下法律法规保护的信息的披露：《美国法典》第 5 编第 2302 (b) (8) 条（适用于违法、浪费、欺诈、滥用、公共卫生或公共安全威胁等信息的披露）、《美国法典》第 5 编第 7211 条（适用于向国会披露）、《美国法典》第 10 编第 1034 条（适用于军方向国会披露）、1947 年《国家安全法》第 1104 条（《美国法典》第 50 编第 3234 条）（适用于情报共同体成员单位的雇员进行的披露）。

(c) 信息来源及获取方法的保护

本章中的任何规定不应被解释为：

(1) 在涉密信息的正确处理、披露或使用方面，影响或豁免联邦政府（或其下属部、局）为了执行相关法律、总统令或程序等而提起的诉讼。

(2) 影响授权执法行动或情报活动的实施。

(3) 为保护涉密信息及其来源和获取方法，以及保护美国国家安全，而更改联邦部、局的权限。

(d) 与其他法律的关系

本章中的任何规定不应被解释为，在非联邦实体向联邦政府提供信息方面，相关法律法规中的任何已有要求会受到影响。

(e) 禁止行为

本章中的任何规定不应被解释为，允许以下行为：价格垄断、在竞争者间分配市场、垄断市场或试图垄断市场、联合拒购、交换价格或成本信息、交换客户名单或交换有关未来竞争规划的信息。

(f) 信息共享关系

本章中的任何规定不应被解释为：

(1) 限制或改变当前的信息共享关系。

(2) 禁止建立新的信息共享关系。

(3) 要求任何非联邦实体与联邦实体或其他非联邦实体，建立新的信息共享关系。

(4) 要求使用根据第 105 条 (c) 款制定的国土安全部内部职能和流程。

(g) 保留合同权利及义务

本章中的任何规定不应被解释为：

(1) 修订、废止或取代任何现行的或即将履行的合同、服务协议条款，或任何非联邦实体之间、非联邦实体与联邦实体之间的其他合约关系；

(2) 或废除任何非联邦实体或联邦实体在商业秘密或知识产权保护方面的权利。

(h) 反分派任务限制

本章中的任何规定不应被解释为，允许联邦实体：

(1) 强制要求非联邦实体向联邦实体或其他非联邦实体提供信息。

(2) 根据非联邦实体与联邦实体或其他非联邦实体共享网络威胁迹象信息的情况，确定是否与其共享网络威胁迹象信息。

(3) 根据非联邦实体与联邦实体或其他非联邦实体共享网络威胁迹象信息的情况，授予其联邦拨款、合同或采购。

(i) 不参与者免责说明

本章中的规定应被解释为，即使不参与本章授权的自愿性活动，实体也无须承担任何责任。

(j) 信息的使用与留存

本章中的任何规定不应被解释为，授权或更改联邦政府部、局的现有权限，允许其在本章许可范围之外使用或留存共享信息。

(k) 联邦优先权

(1) 一般规定——当各州或其行政分支机构的法律法规，对本章授权活动产生了限制或其他特别约束时，按本章规定执行。

(2) 各州法律实施——本章中的任何规定不应被解释为，在授权法律实施惯例和程序方面，取代各州或其行政分支机构的法律法规。

(1) 监管权

本章中的任何规定不应被解释为：

(1) 在未获得本章专门授权批准的情况下，授权颁布任何法规。

(2) 设立或限制本章规定范围之外的任何监管权限。

(3) 授权任何监管措施，造成与其他监管要求、强制性标准，或根据联邦其他法律规定制定的相关流程相重复或冲突的情况。

(m) 国防部部长响应国外恶意网络活动的权限

本章中的任何规定不应被解释为，限制《美国法典》第 10 编第 130 (g) 款赋予国防部部长的权限。

(n) 刑事诉讼

当联邦、州、部落或地方法律要求在刑事诉讼案件中披露时，本章中的任何规定不应被解释为，阻止对共享网络威胁迹象信息或防护措施的披露。

## 第 109 条 网络安全威胁报告

### (a) 报告

本法颁布之日起 180 日内，国家情报总监应与情报共同体中适宜成员单位的负责人协商，向参议院特别情报委员会、众议院常设特别情报委员会提交一份报告，描述网络安全威胁情况，包括网络攻击、网络盗窃和数据泄露等。

### (b) 内容

第 (a) 款要求的报告应包含以下内容：

(1) 对美国与其他国家现有情报共享与合作关系的评估，主要是网络安全方面，包括网络攻击、网络盗窃及数据泄露等。这些威胁包括直接针对美国的，或是可能威胁美国国家安全利益、经济和知识产权的。特别应明确此类关系的效用，包括情报共同体中哪些成员单位参与了此类关系，以及此类关系能否继续改进和如何改进。

(2) 一份国家和非国家行为者的清单，列明最可能产生针对美国的网络安全威胁（包括网络攻击、网络盗窃及数据泄露），威胁美国国家安全利益、经济和知识产权的行为者，以及对它们的评估。

(3) 一份说明，描述私营实体如果延迟发送网络安全威胁（包括网络攻击、网络盗窃及数据泄露）通知，那么会使响应和防范职能受到影响的程度。这些职能主要用于美国政府应对或防范直接针对美国私营部门的网络安全威胁。

(4) 对其他技术或职能的评估，主要是用于提高美国防范、应对网络安全威胁（包括网络攻击、网络盗窃及数据泄露）能力的技术或职能。

(5) 对其他技术或实践措施的评估，主要是针对私营部门采用的、能够迅速部署以协助情报共同体防范、应对网络安全威胁的技术或方法。

### (c) 报告形式

第 (a) 款要求的报告，应同时有涉密和非涉密的版本。

### (d) 情报共同体的定义

本条所述“情报共同体”是指，1947 年《国家安全法》第 3 条（《美国法典》第 50 编第 3003 条）所定义的情报共同体。

## 第 110 条 国防部部长传播特定信息的权限所限制的例外情况

尽管有《美国法典》第 10 编第 393 条 (c) (3) 项的限制规定，国防部部长仍可通过符合本章规定而制定或发布的政策、程序和指南，授权共享网络威胁迹象信息或防护措施。

## 第 111 条 生效期限

### (a) 一般规定

本章及本章修正案自本法颁布之日起生效，至 2025 年 9 月 30 日失效，(b) 款另有规定的除外。

### (b) 例外情况

对于在第 (a) 款所述失效日期之前，发生的任何本章授权行动或通过本章授权行动获取

的信息，本章规定仍持续有效。

## 第Ⅱ章 国家网络安全增强（第 201 ~ 229 条）

### 第 A 节 国家网络安全和通信整合中心（第 201 ~ 211 条）

#### 第 201 条 简称

本节可被称为“2015 年国家网络安全保护增强法”。

#### 第 202 条 定义

在本节中：

(1) 有关国会委员会——是指：

(A) 参议院国土安全及政府事务委员会；

(B) 以及众议院国土安全委员会。

(2) 网络安全风险、事件——采用《2002 年国土安全法》第 227 条中的定义。其中，《2002 年国土安全法》第 227 条是指，根据本法第 223 条 (a) (3) 项修订后的第 227 条。

(3) 网络威胁迹象信息、防护措施——采用本法第 102 条中的定义。

(4) 部门——是指国土安全部。

(5) 部长——是指国土安全部部长。

#### 第 203 条 信息共享框架和流程

对经本法第 223 条 (a) (3) 项修订后的《2002 年国土安全法》第 227 条做如下修订：

[1]在第 (a) 款中：

(A) 原第 (3) 项、第 (4) 项依次重新编号为第 (4) 项、第 (5) 项。

(B) 删除原第 (1) 项、第 (2) 项，插入以下条款：

“(1) ‘网络安全风险’是指：

(A) 由于未经授权访问、使用、披露、损害、干扰、修改或破坏等，造成或引发的信息或信息系统威胁、脆弱性或其他相关后果，包括由于恐怖活动造成的相关后果。

(B) 不包括仅违反消费者服务条款或消费者许可协议的行为。

(2) ‘网络威胁迹象信息’及‘防护措施’的定义参见《2015 年网络安全法》第 102 条。

(3) ‘事件’是指未经合法授权实际或即将损害信息系统，或信息系统中信息的完整性、保密性或可用性的事件。”

(C) 删除经本项重新编号后的第 (4) 项末尾的“以及”。

(D) 删除经本项重新编号后的第 (5) 项末尾的句号，改为“；以及”。

(E) 并且在末尾增加以下条款：

“(6) ‘共享’（包括所有属于‘共享’行为的任意组合）是指，提供、接收及传播（包括上述三项的任意组合）。”

[2]在第 (c) 款中：

(A) 第 (1) 项做如下修改：

(i) 在句尾分号前加入“，包括《2015 年网络安全法》第 I 章的实施”。

(ii) 在“网络安全风险”前加入“网络威胁迹象信息、防护措施”。

(B) 在第(3)项中，删除“网络安全风险”，改为“网络威胁迹象信息、防护措施、网络安全风险”。

(C) 在第(5)(A)目中，删除“网络安全风险”，改为“网络威胁迹象信息、防护措施、网络安全风险”。

(D) 在第(6)项中：

(i) 删除“网络安全风险”，改为“网络威胁迹象信息、防护措施、网络安全风险”。

(ii) 删除句尾处的“以及”。

(E) 在第(7)项中：

(i) 删除(A)目句尾处的“以及”。

(ii) 删除(B)目句尾处的句号，改为“；以及”。

(iii) 在(B)目末尾处增加“(C) 共享网络威胁迹象信息和防护措施；”。

(F) 在末尾处增加以下条款：

“(8) 与国际合作方接洽，并与其他适当的机构协商，以：

(A) 围绕以下方面开展合作：网络威胁迹象信息、防护措施、其他与网络安全风险和事件有关的信息。

(B) 增强全球网络安全水平和恢复能力。

(9) 适当情况下，与联邦机构、非联邦实体（包括各关键基础设施部门）以及各州主要市区融合中心共享网络威胁迹象信息、防护措施、其他与网络安全风险和事件有关的信息。

(10) 适当情况下，参与国土安全部组织的全国演习。

(11) 与国土安全部应急通信办公室合作，评价和评估公共安全通信中网络安全事件的后果、脆弱性及威胁信息，以促进公共安全通信安全水平和恢复能力的持续提升。”

[3]在(d)款(1)项中：

(A) 关于第(B)目：

(i) 删除第(i)段中的“以及地方”，改为“，地方，以及部落”。

(ii) 删除第(ii)段中的“；以及”改为“，包括信息共享和分析中心”。

(iii) 在第(iii)段末尾增加“以及”。

(iv) 在末尾增加：“(iv) 私营实体；”。

(B) 删除(D)目句尾的“以及”。

(C) 原第(E)目重新编号为第(F)目。

(D) 在(D)目之后加入以下条款：

“(E) 围绕网络安全风险和事件与各州、地方政府开展合作，且已与中心建立了自愿信息共享关系的实体；以及”。

[4]在第(e)款中：

(A) 关于第(1)项：

(i) 在(A)目中“信息”前加入“网络威胁迹象信息、防护措施，以及”。

(ii) 在(B)目中“相关信息”前加入“网络威胁迹象信息、防护措施，以及”。

(iii) 在(F)目中：

(I) 删除“网络安全风险”，改为“网络威胁迹象信息、防护措施、网络安全风险”。

(II) 删除句尾的“以及”。

(iv) 删除 (G) 目中的“网络安全风险及事件”，改为“网络威胁迹象信息、防护措施、网络安全风险及事件；以及”。

(v) 在末尾处增加：

“(H) 中心指定一家代理机构与非联邦实体联络。”

(B) 关于第 (2) 项：

(i) 删除“网络安全风险”，改为“网络威胁迹象信息、防护措施、网络安全风险”。

(ii) 在“访问”之后加入“或披露”。

(C) 在第 (3) 项末尾句号前加入“，包括与根据第 222 条任命的隐私官协作，以确保中心遵守《2015 年网络安全法》第 105 条 (b) 款及 (d) 款 (5) (C) 目所述特定政策和程序”。

[5]在末尾处增加：

#### **“(g) 自动信息共享”**

(1) 一般规定——根据《2002 年国土安全法》第 103 条 (a) (1) (H) 目任命的副部长，应与本行业及其他利益相关方协商，创建有关职能机构，以利用合适的现有 IT 行业标准和最佳实践，支撑并快速推进本法第 I 章所述网络威胁迹象信息和防护措施自动共享机制的发展、运用及实施。

(2) 年度报告——根据《2002 年国土安全法》第 103 条 (a) (1) (H) 目任命的副部长，应向参议院国土安全与政府事务委员会、众议院国土安全委员会提交年度报告，描述 (1) 项所述职能制定工作的进展和推进情况。上述职能完全实现前，应持续提交此年度报告。

#### **(h) 自愿信息共享程序**

(1) 程序。

(A) 一般规定——出于本条所述网络安全的目的，中心可与任何已同意的非联邦实体建立自愿信息共享关系，与其共享网络威胁迹象信息和防护措施。本款中任何规定不应被解释为，强行要求任何非联邦实体与中心或其他机构建立这种自愿信息共享关系。中心可根据部长的自主决定，通过副部长（根据《2002 年国土安全法》第 103 条 (a) (1) (H) 目任命的），以任何理由（包括认为与其建立这种共享关系的非联邦实体违反了本款规定）终止上述自愿信息共享关系。

(B) 国家安全——部长可自主决定，通过副部长（根据《2002 年国土安全法》第 103 条 (a) (1) (H) 目任命的），以任何理由（包括认为该决定有利于国家安全）拒绝建立本款所述的自愿信息共享关系。

(2) 自愿信息共享关系——在本项中，本条所述自愿信息共享关系可通过以下协议形式落实：

(A) 标准协议——中心应在国土安全部官方网站上提供一份符合本条规定的标准协议，供非联邦实体使用。

(B) 协商协议——当非联邦实体提出要求时，并且中心认为适当的情况下，国土安全部可根据部长的自主决定，通过副部长（根据《2002 年国土安全法》第 103 条 (a) (1)

(H) 目任命的), 与非联邦实体签订符合本条规定的协商协议。

(C) 已有协议——中心与非联邦实体在本款颁布前已签订或已生效的协议, 即使与本款中其他规定或要求不一致, 仍视为符合本款规定。根据《关于网络安全信息共享与合作的联合研发协议》(2014 年 12 月 31 日起生效) 要求, 本款所述协议应包含隐私保护相关内容。本款中的任何规定不应被解释为, 强制要求非联邦实体签订本款所述标准协议或协商协议。

#### (i) 直接汇报

部长应制定相应政策和程序, 确保中心主任可以直接向部长汇报重要的网络安全风险和事件。

#### (j) 国际合作报告

“本项颁布之日起 180 日内及此后定期, 国土安全部部长应向参议院国土安全与政府事务委员会、众议院国土安全委员会提交报告, 说明其根据本条第 (c) (8) 项规定, 与相关国际合作伙伴开展网络安全合作的进展情况。

#### (k) 推广

本法颁布之日起 60 日内, 部长应通过副部长 (根据《2002 年国土安全法》第 103 条 (a)

(1) (H) 目任命的), 做好以下工作:

(1) 向公众宣传如何与中心自愿共享网络威胁迹象信息和防护措施。

(2) 为推进网络威胁迹象信息和防护措施的共享工作, 加大对关键基础设施所有者、运营者的推广力度。

#### (l) 联合脆弱性披露

部长可与本行业和其他利益相关方合作, 制定并遵守用于协调脆弱性披露的国土安全部政策和程序。”

### 第 204 条 信息共享和分析组织

对《2002 年国土安全法》第 212 条 (《美国法典》第 6 编第 131 条) 做如下修订:

(1) 在第 (5) 项中:

(A) 关于第 (A) 目:

(i) 在“关键基础设施”之后, 加入“ , 包括与网络安全风险和事件有关的信息, ”。

(ii) 在“与关键基础设施有关的”之后, 加入“ , 包括网络安全风险和事件, ”。

(B) 关于第 (B) 目:

(i) 在“关键基础设施信息”之后, 加入“ , 包括网络安全风险和事件, ”。

(ii) 在“与关键基础设施有关的”之后, 加入“ , 包括网络安全风险和事件, ”。

(C) 在第 (C) 目中“关键基础设施信息”之后, 加入“ , 包括网络安全风险和事件, ”。

(2) 在末尾处加入:

“(8) 网络安全风险、事件——‘网络安全风险’和‘事件’的定义参见本章第 227 条”。

### 第 205 条 国家响应框架

在经本节第 223 条 (a) (4) 项修订的基础上, 在《2002 年国土安全法》第 228 条结尾处增加:



**“(d) 国家响应框架**

国土安全部部长应与联邦其他有关部、局的负责人协同，根据 (c) 款要求的《国家网络安全事件响应计划》，定期对国土安全部《国家响应框架网络事件附件》进行更新、维护及演练。”

**第 206 条 降低国土安全部数据中心网络安全风险的报告**

本法颁布之日起 1 年内，国土安全部部长应向有关国会委员会提交一份报告，阐述国土安全部建立相应环境以降低数据中心网络安全风险（包括加强系统间隔离以及在上述隔离的分区之间使用不同的安全控制等）的可行性。

**第 207 条 评估**

本法颁布之日起 2 年内，美国联邦政府总审计长应向有关国会委员会提交一份报告，阐述以下内容：

(1) 对国土安全部部长执行本章及本章修正案情况的评估。

(2) 在可行范围内，评估在中心内部以及由此在全国范围内共享下述信息的增长情况：网络威胁迹象信息、防护措施或与网络安全风险及事件有关的信息。其中，中心是指根据《2002 年国土安全法》第 227 条设立的中心，《2002 年国土安全法》第 227 条是指根据本法第 223 条 (a) 项修订后的第 227 条。

**第 208 条 关键基础设施中多个并发的网络事件**

本法颁布之日起 1 年内，根据《2002 年国土安全法》第 103 条 (a) (1) (H) 目（《美国法典》第 6 编第 131 条 (a) (1) (H) 目）任命的副部长，应向有关国会委员会提供制定风险告知计划可行性的相关信息，以应对影响关键基础设施的多个并发网络事件发生的风险，包括可能对其他关键基础设施产生连锁反应的网络事件。

**第 209 条 美国口岸网络安全脆弱性报告**

本法颁布之日起 180 日内，国土安全部部长应向有关国会委员会和参议院商务、科学和交通委员会、众议院交通与基础设施委员会提交一份报告，描述在其认为最容易发生网络安全事件的 10 个美国口岸中的网络安全脆弱性，并提出缓解上述脆弱性的建议。

**第 210 条 新监管权限的禁止事项**

本节或本节修正案中的任何规定不应被解释为，授权国土安全部部长制定和颁布与非联邦实体（不包括各州、地方及部落政府）网络安全相关，且在本法案颁布之前尚未生效的规章或标准。

**第 211 条 提交报告要求的期限**

本法颁布之日起 7 年后，本节规定的任何报告要求均失效。

**第 B 节 联邦网络安全增强（第 221 ~ 229 条）****第 221 条 简称**

本节可被称为“2015 年联邦网络安全增强法”。

## 第 222 条 定义

在本节中：

- (1) 机构——定义参见《美国法典》第 44 编第 3502 条。
- (2) 机构信息系统——采用《2002 年国土安全法》第 228 条中的定义。其中，《2002 年国土安全法》第 228 条是指根据本法第 223 条 (a) (4) 项修订后的第 228 条。
- (3) 有关国会委员会——是指：
  - (A) 参议院国土安全及政府事务委员会；
  - (B) 众议院国土安全委员会。
- (4) 网络安全风险、信息系统——采用《2002 年国土安全法》第 227 条中的定义。其中，《2002 年国土安全法》第 227 条是指根据本法第 223 条 (a) (3) 项修订后的第 227 条。
- (5) 主任——是指美国管理和预算办公室主任。
- (6) 情报共同体——是指《1947 年国家安全法》第 3 条第 (4) 项（《美国法典》第 50 编 3003 (4) 项）所定义的情报共同体。
- (7) 国家安全系统——定义参见《美国法典》第 40 编 11103 条。
- (8) 部长——是指国土安全部部长。

## 第 223 条 联邦网络安全的增强

(a) 一般规定

对《2002 年国土安全法》第 II 章 C 节（《美国法典》第 6 编第 141 条及以下）做如下修订：

- (1) 原第 228 条重新编号为第 229 条。
- (2) 原第 227 条重新编号为第 228 条第 (c) 款，增加第 (4) 项，并调整页面缩进。
- (3) 将此前已改为第 226 条的原第 2 条（关于国家网络安全及通信整合中心），重新编号为第 227 条。
- (4) 在经上述修订后的第 227 条之后，增加如下条款：

### “第 228 条 网络安全计划

(a) 定义

在本条中：

- (1) ‘机构信息系统’是指，由某一机构或者代表某机构的另一实体使用或运行的信息系统。
- (2) ‘网络安全风险’和‘信息系统’的定义参见第 227 条。
- (3) ‘情报共同体’的定义参见《1947 年国家安全法》第 3 条第 (4) 项（《美国法典》第 50 编第 3003 (4) 项）。
- (4) ‘国家安全系统’的定义参见《美国法典》第 40 编第 11103 条。

(b) 入侵评估计划

- (1) 要求——国土安全部部长应与管理和预算办公室主任协作，共同：
  - (A) 制定并执行入侵评估计划，常态化主动检测、识别、驱除机构信息系统中的入侵者；
  - (B) 在必要时更新上述计划。
- (2) 例外情况——第 (1) 项要求的入侵评估计划不适用于国防部、国家安全系统或情报

共同体的相关部门。”

(5) 在经本条第(2)项重新编号后的第228条第(c)款中,删除“第226条”,改为“第227条”。

(6) 在修订后的第229条之后增加如下条款:

#### **“第230条 联邦入侵检测与防护系统**

##### **(a) 定义**

在本条中:

- (1) “机构”的定义参见《美国法典》第44编第3502条。
- (2) “机构信息”是指,由机构或其代表收集或维护的信息。
- (3) “机构信息系统”的定义参见第228条。
- (4) “网络安全风险”和“信息系统”的定义参见第227条。

##### **(b) 要求**

(1) 一般规定——本条颁布之日起1年内,国土安全部部长应部署、运行和维护可供任何机构有偿或无偿使用的:

(A) 一种职能,用于检测经过或流入/流出机构信息系统网络流量的网络安全风险;

(B) 一种职能,用于阻止具有网络安全风险的网络流量经过或流入/流出机构信息系统,或调整该网络流量以消除网络安全风险。

(2) 常规改进——国土安全部部长应经常在(1)项所述入侵检测与防护职能中应用新技术或调整现有技术,以改进该职能。

##### **(c) 活动**

在执行(b)款规定的过程中:

(1) 部长或根据第(2)项规定为部长提供协助的私营实体,可访问(无论在何处访问)经过或流入/流出机构信息系统的信息,即使其他法律有限制或禁止该机构负责人披露的规定,该机构负责人仍可向部长或根据第(2)项规定为部长提供协助的私营实体披露上述信息。

(2) 部长可与私营实体签订合同或其他协议,或要求并获得私营实体的协助,以部署、运行、维护(b)款所述技术。

(3) 仅当保护信息和信息系统免受网络安全风险侵害时,部长方可留存、使用以及披露通过本条授权活动获取的信息。

(4) 部长应经常在真实和模拟环境中开展测试和评估,评估可用的高级保护技术(包括商业、非商业技术以及基于签名检测技术之外的其他检测技术),以改进检测和防护职能,并于适当时获取、测试和部署此类技术。

(5) 部长应设立试点项目,以尽快获取、测试和部署第(4)项所述技术。

(6) 部长应定期更新《2002年电子政务法》第208条(b)款(《美国法典》第44编第3501条注释)要求的隐私影响评估。

##### **(d) 原则**

在(b)款的执行过程中,国土安全部部长应确保:

(1) 出于保护机构信息及信息系统免受网络安全风险影响的合理、必要目的,实施本条所述活动。

(2) 部长获取信息的留存期限,不得超过保护机构信息及信息系统免受网络安全风险影响所需的合理、必要期限。

(3) 在出于保护机构信息及信息系统的目的，访问机构信息系统用户通信时，需提前通知用户。

(4) 上述活动的实施，要符合用于管理入侵检测与防护职能运行的政策和程序。

#### **(e) 私营实体**

(1) 条件——(c) 款第(2) 项所述私营实体，不得：

(A) 将经过或流入/流出某一机构信息系统的任何网络流量（包括与网络安全风险无直接关系的具体人员个人信息或能识别具体人员的信息），披露给国土安全部或根据(c) 款第(1) 项要求向国土安全部披露该信息的机构之外的任何实体。

(B) 使用其已根据本条规定获得了访问权限的经过或流入/流出联邦机构信息系统的任何网络流量，除非是为了保护联邦机构信息及机构信息系统免受网络安全风险影响，或执行根据第(c) 款第(2) 项签订的合同或协议以及与部长签订的其他协议条款。

(2) 责任范围——在符合本条规定或依照(c) 款第(2) 项签订的合同或协议要求的前提下，私营实体不应因向国土安全部部长提供协助而在任何法院受到起诉。

(3) 说明——第(2) 项中的任何规定不应被解释为，授权互联网服务供应商，在未经消费者同意的情况下，违反与消费者签订的用户协议。

#### **(f) 隐私官审查**

本条颁布之日起1 年内，根据本法第222 条任命的隐私官应与司法部部长协商，对根据本条制定的政策和指南进行审查，以确保其符合其他适用的隐私法，包括管理通信获取、拦截、保留、使用和披露行为的法律。”

#### **(b) 机构职责**

(1) 一般规定——除第(2) 项规定的情况外：

(A) 本法颁布之日起1 年内，或国土安全部部长根据《2002 年国土安全法》第230 (b)(1) 项（经本条第(a) 款修订的）规定，制定入侵检测与防护职能之日起2 个月内（取日期较晚者），各机构负责人应针对机构信息系统同该系统之外任何其他信息系统之间传输的信息，采用并持续使用上述职能。

(B) 国土安全部部长根据《2002 年国土安全法》第230 (b)(2) 项（经本法第(a) 款修订的）规定，改进入侵检测与防护职能之日起6 个月内，各机构负责人应采用并持续使用改进后的入侵检测与防护职能。

(2) 例外情况——第(1) 项的要求不适用于国防部、国家安全系统或情报共同体的相关部门。

(3) 定义——尽管第222 条另有规定，但在本款中，“机构信息系统”是指某一机构拥有或运行的信息系统。

(4) 说明——本条中的任何规定不应被解释为，限制一个机构根据其负责人的自主决定或其他相关政策、政令和指南，在经本法第(a) 款修订的《2002 年国土安全法》第230 (b)(1) 项所述信息系统之外的其他信息系统中应用入侵检测与防护职能。

#### **(c) 目录修订**

对《2002 年国土安全法》第1 (b) 款（《美国法典》第6 编第101 条注释）中的目录做如下修订：

删除与已修订为第226 条的原第1 条有关的内容，删除与已修订为第226 条（关于国家网络安全和通信整合中心）、第227 条、第228 条的原第2 条有关的内容，加入以下条目：

- “第 226 条 网络安全人员招聘与留用”；  
“第 227 条 国家网络安全和通信整合中心”；  
“第 228 条 网络安全计划”；  
“第 229 条 调查”；  
“第 230 条 联邦入侵检测与防护系统”。

#### 第 224 条 高级内部防御

##### (a) 高级网络安全工具

(1) 一般规定——在国土安全部一直以来诊断和降低网络安全风险的一系列工作之中，部长应引入高级网络安全工具（包括付费工具、免费工具或开源工具），以提高网络活动的可视性，检测和减少入侵和异常活动。

(2) 计划的制定——管理和预算办公室主任应当制定一项计划，并由国土安全部部长负责实施，以确保各机构能够运用高级网络安全工具（包括第（1）项所述工具）来检测和减少入侵和异常活动。

##### (b) 高级安全工具的优先级

管理和预算办公室主任、国土安全部部长应与有关机构协商，以：

(1) 审查并更新联邦政府的政策和项目，以确保网络安全监控工具在机构网络内得到了恰当应用，并拥有合适的使用优先级。

(2) 向有关国会委员会简要汇报上述优先使用情况。

##### (c) 改进评估指标

国土安全部部长应与管理和预算办公室主任合作，审查并更新《美国法典》第 44 编第 3554 条所述安全性评估指标，使其包含对入侵和事件的检测时间和响应时间的度量。

##### (d) 透明性与责任

管理和预算办公室主任应与国土安全部部长协商，通过在联邦政府绩效网站上增加更多的安全性评估指标，并在可行范围内最大程度地向各部门的组成机构及小型、微型机构明示，提高机构网络安全态势对公众的透明度。

##### (e) 技术维护

对《美国法典》第 44 编第 3553 (b) (6) (B) 目做如下修订：在“部署”之后插入“，运营与维护”。

##### (f) 例外情况

本条规定不适用于国防部、国家安全系统以及情报共同体的相关机构。

#### 第 225 条 联邦网络安全要求

##### (a) 联邦网络安全标准的实施

根据《美国法典》第 44 编第 3553 条的规定，国土安全部部长应与管理和预算办公室主任协商行使部长权限，发布具有约束力的操作指令，在确保各机构及时采用并遵守根据《美国法典》第 40 编第 11331 条颁布的政策和标准方面，为管理和预算办公室主任提供帮助，进而保护各机构信息系统安全。

##### (b) 机构的网络安全要求

(1) 一般规定——除本款第（2）项规定的情况外，本法颁布之日起 1 年内，各机构负责

人应根据《美国法典》第 44 编第 35 节第 II 部分信息安全相关政策、标准、指南和指令，以及依据《美国法典》第 40 编第 11331 条发布的标准和指南，执行以下事项：

(A) 根据《美国法典》第 44 编第 3505 条第 (c) 款第 1 部分（主信息系统清单），和第 2 部分（信息系统清单）中要求的清单，识别该机构存储的敏感数据和关键业务数据。

(B) 评估第 (A) 目所述数据的访问控制措施、对数据存储易访问性的需求，以及个人访问数据的需求。

(C) 使用加密或其他方式，使未授权用户难以破译该机构信息系统存储或传输的第 (A) 目所述数据。

(D) 对需要进行用户身份验证的各机构公共网站，应使用总务管理局局长与国土安全部部长协同开发的单点登录可信身份平台，供个人用户访问时使用。

(E) 根据《2014 年网络安全增强法》第 504 条（公法编号 113-274；《美国法典》第 15 编第 7464 条），对下列事项实施身份管理，包括多因子认证：

(i) 机构信息系统的远程访问；

(ii) 机构信息系统中已提升权限的用户账号。

(2) 例外情况——第 (1) 项规定不适用于以下的机构信息系统：

(A) 该机构的负责人已亲自向管理和预算办公室主任提交了如下证明：

(i) 证明中列出的运行要求及与机构信息系统相关的其他要求会造成该系统负载过重，而无法执行该网络安全要求。

(ii) 上述网络安全要求并不是保护该机构信息系统或其中存储、传输的机构信息所必需的。

(iii) 该机构已采取了一切必要措施，以保护机构信息系统及其中存储、传输的机构信息的安全。

(B) 并且该机构负责人或其指定人员，已向有关国会委员会和该机构的授权委员会提交了第 (A) 目要求的证明。

(3) 说明——本条中的任何规定均不应解释为：更改国土安全部部长、管理和预算办公室主任或国家标准与技术研究院院长关于执行《美国法典》第 44 编第 35 节第 II 部分规定的权限；影响国家标准与技术研究院的标准流程或《美国法典》第 44 编第 3553 (a) (4) 项的其他要求；阻止持续改进和完善用以促进联邦信息安全的技术、标准、政策和指南。

(c) 例外情况

本条的规定不适用于国防部、国家安全系统以及情报共同体的相关机构。

## 第 226 条 评估和报告

(a) 定义

在本条中：

(1) 机构信息——采用《2002 年国土安全法》第 230 条中的定义。其中，《2002 年国土安全法》第 230 条是指经本法第 223 条 (a) (6) 项修订后的第 230 条。

(2) 网络威胁迹象信息、防护措施——定义参见本法第 102 条。

(3) 入侵评估——是指根据入侵评估计划，为识别并驱除机构信息系统中的入侵者所采取的行动。

(4) 入侵评估计划——是指《2002 年国土安全法》第 228 条第 (b) (1) 项要求的计划。其中，《2002 年国土安全法》第 228 条是指经本法第 223 条 (a) (4) 项修订后的第 228 条。

(5) 入侵检测与防护职能——是指《2002 年国土安全法》第 230 条第 (b) 款要求的职能。其中，《2002 年国土安全法》第 230 条是指经本法第 223 条 (a) (6) 项修订后的第 230 条。

#### (b) 第三方评估

本法颁布之日起 3 年内，针对联邦政府为保护机构信息系统所制定方案和战略（包括入侵检测与防护职能、入侵评估计划），总审计长应进行有效性研究，并发布研究报告。

#### (c) 报送国会的报告

##### (1) 入侵检测与防护职能。

(A) 国土安全部部长报告——本法颁布之日起 6 个月内以及此后每年，国土安全部部长应向有关国会委员会提交报告，说明入侵检测与防护职能的实施情况，报告内容应包括：

(i) 对隐私保护控制措施的说明。

(ii) 对检测网络流量中的网络安全风险而采用的技术与职能的说明，包括其对现有商业性和非商业性技术的使用程度。

(iii) 对阻止具有网络安全风险的网络流量经过、流入/流出机构信息系统而采用的技术与职能的说明，包括其对现有商业性和非商业性技术的使用程度。

(iv) 一份清单，描述在各版入侵检测与防护职能中，针对经过、流入/流出机构信息系统的网络流量，用于检测网络安全风险的迹象信息、标识、技术的类型，以及每类中包含的迹象信息、标识和技术的数量。

(v) 在经过、流入/流出机构信息系统的网络流量中，入侵检测与防护职能检测到网络安全风险的次数，及成功阻拦具有网络安全风险的网络流量的次数。

(vi) 根据《2002 年国土安全法》第 230 条第 (c) (5) 项所设试点的说明，包括测试新技术的数量和参与机构的数量。其中，《2002 年国土安全法》第 230 条是指根据本法第 223 条 (a) (6) 项修订后的第 230 条。

(B) 管理和预算办公室报告——本法颁布之日起 18 个月内以及此后每年，管理和预算办公室主任应向国会提交一份应用分析说明，作为《美国法典》第 44 编第 3553 (c) 款所要求报告的一部分，描述各机构对入侵检测与防护职能的应用情况。报告内容应包括：

(i) 一份清单，列明在信息系统中应用入侵检测与防护职能的机构名录，及其应用的程度。

(ii) 一份清单，按机构列明：

(I) 针对经过、流入/流出机构信息系统网络流量，入侵检测与防护职能检测到网络安全风险的次数，以及迹象信息、风险的标识特征和所使用技术类型。

(II) 针对含有网络安全风险的网络流量经过、流入/流出机构信息系统，入侵检测与防护职能成功阻拦的次数，以及迹象信息、风险的标识特征和所使用技术类型。

(C) 首席信息官报告——本法颁布之日起 18 个月至 2 年内，联邦首席信息官应编制一份报告，评估入侵检测与防护职能，并向有关国会委员会提交。报告内容应包括：

(i) 在识别、阻断和防范针对机构信息及机构信息系统的各种网络威胁因素（包括高级持续威胁）方面，系统的有效性。

(ii) 入侵检测与防护职能、持续诊断与风险缓解机制及其他根据《2002 年国土

安全法》第Ⅱ章 D 节（《美国法典》第 6 编第 231 条及以下条款）部署的系统，能否有效保护联邦信息系统。

（iii）入侵检测与防护功能的成本与效益，包括与商用技术和工具的对比，以及涉密网络威胁迹象信息的价值。

（iv）当敏感网络威胁迹象信息和防护措施通过用于商用技术和工具的非涉密机制进行共享时，各机构对他们的保护能力。

（2）管理和预算办公室关于制定和实施入侵评估计划、高级内部防御及联邦网络安全要求的报告——主任应：

（A）于本法颁布之日起 6 个月内，及本法发布任何更新后 30 日内，向有关国会委员会提交入侵评估计划。

（B）于本法颁布之日起 1 年内及此后每年，作为《美国法典》第 44 编第 3553（c）款所要求报告的一部分，将下列事项提交至国会：

（i）一份关于入侵评估计划执行情况的说明；

（ii）根据入侵评估计划，实施入侵评估的成果；

（iii）根据第 224（a）（1）项规定，为持续诊断和缓解网络安全风险而采用的高级网络安全工具的说明；

（iv）一份清单，按机构列明第 225（b）款规定的符合情况。

（C）并且于本法颁布之日起 1 年内，向有关国会委员会提交下列材料：

（i）根据本法第 224（a）（2）项所制定计划的副本；

（ii）根据本法第 224（c）款所制定的改进评价指标。

（d）形式

本条要求的报告应以非涉密形式提交，但可包含涉密附件。

## 第 227 条 终止

（a）一般规定

《2002 年国土安全法》第 230 条所赋予的权力以及本法第 226（c）款提出的报告要求，均自本法颁布之日起 7 年后终止。其中，《2002 年国土安全法》第 230 条是指根据本法第 223 条（a）（6）项修订后的第 230 条。

（b）说明

（a）款中的任何规定不应被解释为可以影响私营实体下述行为的责任范围：在（a）款规定的终止日期前或在授权期间，根据《2002 年国土安全法》第 230（d）（2）项规定向国土安全部部长提供协助。其中，《2002 年国土安全法》第 230 条是指根据本法第 223 条（a）（6）项修订后的第 230 条。

## 第 228 条 国家安全相关信息系统的识别

（a）一般规定

除（c）款中另行规定的事项外，本法颁布之日起 180 日内：

（1）国家情报总监与管理和预算办公室主任应协同其他机构的负责人：

（A）识别所有符合下述条件的非涉密信息系统：可使敌方通过访问该系统中的信息，获取推演其他涉密信息的能力。



(B) 针对第 (A) 目识别出的非涉密信息系统, 评估其可能面临的风险。

(C) 如果第 (A) 目识别出的非涉密信息系统被认定为国家安全系统, 评估这种转变对系统所属机构执行相关任务带来的开销和影响。

(2) 国家情报总监与管理与预算办公室主任应向有关国会委员会、参议院特别情报委员会、众议院常设特别情报委员会提交一份报告, 描述执行第 (1) 项的成果。

(b) 形式

第 (a) (2) 项规定的报告应以非涉密形式提交, 且应包含一份涉密附件。

(c) 例外情况

第 (a) (1) 项的规定不适用于国防部、国家安全系统或情报共同体的相关机构。

(d) 说明

本条中的各项规定不应被解释为可以指定某信息系统为国家安全系统。

## 第 229 条 机构指引

(a) 一般规定

修订《美国法典》第 44 编第 3553 条, 在其结尾处增加以下条款:

### “(h) 机构指引

(1) 权限

(A) 一般规定——在符合第 (B) 目规定的情况下, 为响应机构信息安全面临的已知或疑似信息安全威胁、脆弱性或产生严重威胁的事件, 保护该信息系统免受或减轻信息安全威胁, 国土安全部部长可向机构负责人发布紧急指令, 对收集、处理、存储、传输、传播或留存机构信息的信息系统 (包括由代表该机构的其他实体使用或运行的系统) 的运行采取任何合法行动。

(B) 例外情况——本款赋予部长的权限不适用于第 (d) 款所述系统、第 (e) (2) 项或第 (e) (3) 项所述系统。

(2) 行使权限的程序——部长应:

(A) 协同管理和预算办公室主任, 适当时与联邦合同商协商, 制定相应程序, 管理根据本款要求发布指令的情形, 程序内容应包括:

(i) 阈值及其他标准;

(ii) 隐私和公民自由保护措施;

(iii) 向可能受到影响的第三方发出通知。

(B) 具体说明需要采取措施的原因以及指令的有效期限。

(C) 通过下述措施, 使本款规定的指令所造成的影响最小化:

(i) 在能够保护机构信息系统安全的基础上, 采取最低程度的侵入性措施。

(ii) 为指令制定其所需的最短期限。

(D) 发布本款规定的指令时, 立即通知管理和预算办公室主任和所有受影响机构的负责人。

(E) 如果任何指令应用了国家标准与技术研究院制定的标准和指南, 则与院长进行商讨。

(F) 确保依据本款发布的指令与根据《美国法典》第 40 编第 11331 条发布的标准和指南不冲突。

(G) 参考由国家标准与技术研究院制定, 并由商务部部长根据《美国法典》第 40 编

第 11331 条规定发布的各项适用的标准或指南。

(H) 每年 2 月 1 日前, 向有关国会委员会提交一份报告, 说明部长按第 (1) (A) 目规定所采取的具体行动。

(3) 紧急威胁

(A) 一般规定——尽管《美国法典》第 3554 条另有规定, 在下列情况下, 为了保护机构信息系统安全, 国土安全部部长仍可根据本款规定, 授权使用依《2002 年国土安全法》第 230 (b) (1) 项建立的入侵检测与防护职能:

(i) 部长确定机构信息系统存在紧急威胁。

(ii) 部长确定, 根据第 (b) (2) (C) 目或第 (b) (1) (A) 目发布的指令可能无法及时响应安全威胁。

(iii) 经合理推测, 部长确定, 紧急威胁带来的风险远大于在其控制下实施入侵检测与防护职能可能造成的不利影响。

(iv) 部长事先通知管理和预算办公室主任、依据本项将对其采取具体措施的各机构负责人及首席信息官 (或类似职责的官员), 并于采取措施的 7 日内将下列事项通知有关国会委员会和上述各机构的授权委员会:

(I) 依据本项采取的任何措施。

(II) 采取上述措施的原因、期限及性质。

(v) 部长采取的措施符合其他适用法律的规定。

(vi) 部长根据第 (C) 目制定的预定程序, 授权使用入侵检测与防护职能。

(B) 委托限制——国土安全部部长不得将本项赋予的权限委托他人代为行使。

(C) 预定程序——对可根据第 (A) 目规定授权使用入侵检测与防护职能的情况, 部长应协同管理和预算办公室主任, 并与联邦机构负责人协商, 制定相应程序加以管理, 并将该程序提交至国会。

(4) 限制——仅在下列情况下, 国土安全部部长可根据本款规定指示或授权使用入侵检测与防护职能或执行其他合法行动:

(A) 保护机构信息免受未授权的访问、使用、披露、干扰、修改或破坏。

(B) 或针对以下事项, 需要修复或防御已确定的信息安全风险:

(i) 由机构或者其代表机构收集或维护的信息。

(ii) 由机构、机构合同商或代表该机构的其他组织, 使用或运行的信息系统的一部分。

(i) 提交给国会的年度报告

每年 2 月 1 日前, 管理和预算办公室主任与国土安全部部长应向有关国会委员会提交一份报告, 说明他们根据第 (a) (5) 项及《美国法典》第 44 编第 11303 (b) (5) 项所采取的具体措施。

(j) 有关国会委员会的定义

在本条中, “有关国会委员会” 是指:

(1) 参议院拨款委员会、参议院国土安全与政府事务委员会。

(2) 众议院拨款委员会、众议院国土安全委员会、众议院监管与政府改革委员会, 及众议院科学、空间与技术委员会;”。

**(b) 统一修订**

对《美国法典》第 44 编第 3554 (a) (1) (B) 目做如下修订：

(1) 删除第 (iii) 段末尾的“以及”。

(2) 在结尾处增加如下条款：

“(v) 国土安全部部长根据第 3553 条第 (h) 款签发的紧急指令；以及”。

**第三章 联邦网络安全人员评价（第 301 ~ 305 条）****第 301 条 简称**

本节可被称为“2015 年联邦网络安全人员评价法”。

**第 302 条 定义**

在本节中：

(1) 有关国会委员会——是指：

- (A) 参议院军事委员会；
- (B) 参议院国土安全与政府事务委员会；
- (C) 参议院特别情报委员会；
- (D) 参议院商业、科学和交通委员会；
- (E) 众议院军事委员会；
- (F) 众议院国土安全委员会；
- (G) 众议院监管与政府改革委员会；
- (H) 众议院常设特别情报委员会。

(2) 主任——是指人事管理办公室（OPM）主任。

(3) 国家网络安全教育计划——是指经《2014 年网络安全增强法》第 401 条（《美国法典》第 15 编 7451 条）授权的国家网络安全意识与教育项目所规定的计划。

(4) 工作角色——是指需要专业知识、技能和能力的特定任务及职能的组合。

**第 303 条 国家网络安全人员评价计划**

(a) 一般规定

各联邦机构负责人应：

- (1) 确定机构内需要网络安全或其他网络相关功能的所有岗位；
- (2) 依据国家网络安全教育计划和第 (b) 款的规定，分配对应的职业代码。

(b) 职业代码

(1) 程序

(A) 代码结构——本法颁布之日起 180 日内，人事管理办公室主任应协同国家标准与技术研究院，依据国家网络安全教育计划制定代码结构。

(B) 文职网络人员的确认——本法颁布之日起 9 个月内，人事管理办公室主任应协同国土安全部部长、国家标准与技术研究院院长和国家情报总监，建立国家网络安全教育计划代码结构实施流程，以确认需要网络安全或其他网络相关功能的所有联邦文职岗位。

(C) 非文职网络人员的确认——本法颁布之日起 18 个月内，国防部长应建立相应程序，实施国家网络安全教育计划代码结构，以确认需要网络安全或其他网络相关功能的所有联邦非文职岗位。

(D) 现有网络安全人员的基线评价——第 (B) 目和第 (C) 目规定的流程建立之日起 3 个月内，各联邦机构负责人均应向具有管辖权的有关国会委员会提交一份报告，说明：

(i) 当前从事信息技术、网络安全或其他网络相关工作，且持有行业认可证书的人员比例，如国家网络安全教育计划确认的证书；

(ii) 其他尚未持有证书的文职和非文职网络人员参加认证考试的准备水平；

(iii) 通过为现有人员提供适宜的培训和认证，缩小第 (i) 段和第 (ii) 段所述之间差距的战略。

(E) 代码分配程序——第 (B) 目和第 (C) 目规定的程序建立之日起 3 个月内，各联邦机构负责人应建立以下程序：

(i) 确认涉及信息技术、网络安全或其他网络相关功能（依据国家网络安全教育计划定义的）的冗余岗位和空缺岗位；

(ii) 依据认可的标准和定义，为上述岗位分配职业代码。

(2) 代码分配——第 (1) 项第 (E) 目所述程序建立之日起 1 年内，各机构负责人应针对本机构内涉及信息技术、网络安全或其他网络相关功能的岗位，完成职业代码分配。

(c) 进度报告

本法颁布之日起 180 日内，人事管理办公室主任应向有关国会委员会提交一份进度报告，说明本条的实施情况。

### **第 304 条 具有关键需求的网络相关工作角色的确定**

(a) 一般规定

根据第 303 条第 (b) 款第 (2) 项为员工分配职业代码之日起 1 年内，且于此后每年（直至 2022 年），各联邦机构负责人应与人事管理办公室主任、国家标准与技术研究院院长和国土安全部部长协商：

(1) 确认该机构的工作人员中，具有关键需求的信息技术、网络安全或其他与网络相关工作角色。

(2) 向人事管理办公室主任提交报告，包括：

(A) 描述本条第 (1) 项所确认的信息技术、网络安全或其他与网络相关角色；

(B) 证实所述工作角色的关键需求。

(b) 指导

人事管理办公室主任应及时向联邦机构提供指导，以确认具有关键需求的信息技术、网络安全或其他网络相关角色，包括：

(1) 当前存在严重技术短板的信息技术、网络安全或其他与网络相关角色；

(2) 存在新兴技术短板的信息技术、网络安全或其他与网络相关角色。

(c) 网络安全需求报告

本法颁布之日起 2 年内，人事管理办公室主任应与国土安全部部长协商：

(1) 确认所有联邦机构对信息技术、网络安全或其他与网络相关工作人员的关键需求；

- (2) 向有关国会委员会提交一份进度报告，说明本条的实施情况。

#### 第 305 条 政府问责办公室进展报告

美国审计总长应：

- (1) 分析和监测第 303 条和第 304 条的实施情况；  
(2) 本法颁布之日起 3 年内，向有关国会委员会提交一份报告，说明上述实施情况。

### 第 IV 章 其他网络事项（第 401 ~ 407 条）

#### 第 401 条 移动设备安全研究

##### (a) 一般规定

本法颁布之日起 1 年内，国土安全部部长应与国家标准与技术研究院院长协商：

- (1) 完成联邦政府内移动设备安全威胁的相关研究工作。  
(2) 向国会提交一份非涉密报告，必要时可附上涉密附件。报告应包含上述研究成果、根据第 (b) (3) 项提出的相关建议、根据第 (b) (5) 项制定的计划，以及根据第 (b) (4) 项确定的缺陷（如果存在）。

##### (b) 研究内容

在第 (a) 款第 (1) 项的研究过程中，国土安全部部长应同国家标准与技术研究院院长协商：

- (1) 以台式计算机为基础，评估移动安全技术的发展过程，以及这些技术是否足以应对当前的移动安全挑战。  
(2) 评估上述威胁对联邦政府信息系统和互联网（不包括国家安全系统以及国防部和情报共同体的信息系统和网络）的网络安全，可能造成的影响。  
(3) 基于行业标准和最佳实践措施，提出处理上述威胁的相关建议。  
(4) 在国土安全部部长的现有权限范围内，识别出妨碍其处理联邦政府移动设备安全问题（不包括国家安全系统、国防部和情报共同体的信息系统和网络）的缺陷。  
(5) 制定促进国土安全部采用安全移动设备技术的计划。

##### (c) 情报共同体的定义

本条中“情报共同体”的定义参见《1947 年国家安全法》第 3 条（《美国法典》第 50 编第 3003 条）。

#### 第 402 条 国务院国际网络空间政策战略

##### (a) 一般规定

本法颁布之日起 90 日内，国务卿应制定有关美国网络空间国际政策的综合战略。

##### (b) 战略要素

第 (a) 款所要求的战略应包含以下内容：

- (1) 为支持以下目标，国务卿采取的措施和活动的总结：2011 年 5 月，总统签署《网络空间国际战略》，目标是通过国际合作，构建开放、互操作、安全、可靠的信息通信基础设施，以促进国际贸易与商业发展、加强国际安全、鼓励言论自由和自主创新。

(2) 指导国务卿外交活动的行动计划, 包括为制定国际网络行为规范而举行的双边和多边活动, 并总结当前多边论坛为推动国际网络行为规范达成共识而进行讨论。

(3) 总结各主要国家针对国际网络行为规范提出的不同概念, 包括中国、俄罗斯、巴西、印度。

(4) 详述网络空间中其他国家、受国家资助的人和个人对美国国家安全造成的威胁, 包括美国联邦和私营部门基础设施、知识产权及公民隐私等。

(5) 总结总统可用于阻止其他国家、受国家资助的人和个人的政策手段, 包括 2015 年 4 月 1 日签发的第 13694 号总统行政令中列举的事项。

(6) 总结国务卿和网络事务协调员办公室为建立国际网络行为规范所需要的相关资源。

(c) 协商

在第 (a) 款所述战略的制定过程中, 适当时, 国务卿应与美国其他机构和部门以及在对外政策、国家安全与网络安全方面持有相关资质证明、拥有特定专长的私营部门和非政府组织进行协商。

(d) 战略形式

第 (a) 款所述战略, 应以非涉密的形式给出, 但可包含涉密附件。

(e) 信息发布

国务卿应:

(1) 公开发布第 (a) 款所述战略;

(2) 向参议院对外关系委员会、众议院对外事务委员会简要汇报该战略, 包括涉密附件的内容。

#### **第 403 条 国际网络犯罪分子的逮捕与起诉**

(a) 国际网络犯罪分子的定义

本条中, “国际网络犯罪分子” 是指:

(1) 确信已参与侵犯美国国家利益或公民权益的网络犯罪或知识产权犯罪的人员;

(2) 下列人员:

(A) 已由美国法官签发逮捕令的人员;

(B) 或者已由国际刑警组织发布国际通缉令的人员 (通常指红色通缉令)。

(b) 非合作性协商

因未与美国签订引渡协议或其他原因, 在某些国家难以进行引渡, 但在这些国家确实存在一名或多名国际网络犯罪分子, 国务卿或其指定人员应与这些国家政府官员进行协商, 以确定该国政府采取的措施, 包括以下方面:

(1) 逮捕、起诉此类犯罪分子;

(2) 阻止此类犯罪分子实施侵犯美国国家利益或公民权益的网络犯罪或知识产权犯罪。

(c) 年度报告

(1) 一般规定——国务卿应向有关国会委员会提交年度报告, 包括以下内容:

(A) 按国家列明其他国家内国际网络犯罪分子的数量, 并标明未与美国签订引渡协或其他原因而无法实施引渡的国家。

(B) 围绕制止或起诉国际网络犯罪分子, 国务院官员与外国官员举行重要会谈的类别

和次数，包括这些国家的名称。

(C) 以及上一自然年内，引渡至美国的国际网络犯罪分子的下列信息：

- (i) 姓名；
- (ii) 被指控的罪名；
- (iii) 原居住国；
- (iv) 从哪个国家引渡至美国。

(2) 形式——本款所要求的报告应最大程度地采取非涉密形式，但可包含涉密附件。

(3) 有关国会委员会——出于本款规定的目的，“有关国会委员会”是指：

(A) 参议院对外关系委员会，参议院拨款委员会，参议院国土安全与政府事务委员会，参议院银行、住房和城市事务委员会，参议院特别情报委员会以及参议院司法委员会；

(B) 众议院对外事务委员会、众议院拨款委员会、众议院国土安全委员会、众议院金融服务委员会以及众议院常设特别情报委员会。

#### 第 404 条 应急服务增强

##### (a) 数据收集

本法颁布之日起 90 日内，国土安全部部长应协同有关联邦实体和应急通信办公室主任，通过依《2002 年国土安全法》第 227 条规定所建立的国家网络安全和通信整合中心，建立相关流程，确保各州互操作性协调员，针对各州应急响应提供者[参照《2002 年国土安全法》第 2 条（《美国法典》第 6 编第 101 条）中的定义]使用的信息系统或互联网，能够报告网络安全风险或事件相关数据。其中，《2002 年国土安全法》第 227 条是指根据本法第 223 条（a）（3）项修订后的第 227 条。

##### (b) 数据分析

本法颁布之日起 1 年内，国土安全部部长应通过国家网络安全和通信整合中心主任协同相关实体和应急通信办公室主任，并通过国家标准与技术研究院院长与商务部部长协商，对本条第（a）款所报告的数据进行整合和分析，从而为各州应急响应提供者使用的信息系统或互联网，提供安全和恢复措施方面的信息与建议。

##### (c) 最佳实践

(1) 一般规定——利用第（b）款给出的数据整合和分析结果以及其他所有相关信息，国家标准与技术研究院院长应通过《国家标准与技术研究院法》第 2 条第（e）款（《美国法典》第 15 编第 272（e）款）所述程序，持续推动和支持相关方法的制定，以减轻应急响应提供者所面临的网络安全风险。

(2) 报告——国家标准与技术研究院院长应向国会提交一份报告，说明第（1）项活动的结果，包括其依据第（1）项提出的方法；同时，应在国家标准与技术研究院网站上进行公布。

##### (d) 说明

本条中的任何规定不应被解释为：

(1) 依据第（a）款的规定要求各州报告数据。

(2) 或者要求非联邦实体（定义参见本法第 102 条）：

(A) 采纳第（b）款提出的建议措施；

(B) 或者遵循第（c）款活动的实施结果，包括本项所述任何方法。

#### 第 405 条 提高医疗卫生行业的网络安全

##### (a) 定义

在本条中：

##### (1) 有关国会委员会——是指：

(A) 参议院卫生、教育、劳动和福利委员会、参议院国土安全与政府事务委员会、参议院特别情报委员会；

(B) 众议院能源和商业委员会、众议院国土安全委员会、众议院常设特别情报委员会。

(2) 业务伙伴——定义参见《美国联邦法规》(在本法制定之日前生效)第 45 章第 160 节第 103 条。

(3) 适用实体——定义参见《美国联邦法规》(在本法制定之日前生效)第 45 章第 160 节第 103 条。

(4) 网络安全威胁、网络安全威胁迹象信息、防护措施、联邦实体、非联邦实体、私营实体——定义参见本法第 102 条。

(5) 医疗卫生票据交换中心、医疗卫生服务提供者、卫生计划——定义参见《美国联邦法规》(在本法制定之前生效)第 45 章第 160 节第 103 条。

##### (6) 医疗卫生行业利益相关方——是指：

(A) 卫生计划、医疗卫生票据交换中心或医疗卫生服务提供者；

(B) 患者或消费者利益倡导者；

(C) 药剂师；

(D) 医疗信息技术的开发者或供应商；

(E) 实验室；

(F) 医药或医疗设备制造商；

(G) 或者为满足第 (b) (1) 项、第 (c) (1) 项、第 (c) (3) 项或第 (d) (1) 项的目的，部长认为必要的其他利益相关方。

(7) 部长——是指健康和公众服务部部长。

##### (b) 报告

(1) 一般规定——本法颁布之日起 1 年内，健康和公众服务部部长应向参议院卫生、教育、劳动和福利委员会及众议院能源和商业委员会提交一份报告，说明本部门和医疗卫生行业利益相关方为应对网络安全威胁所做的准备。

(2) 报告内容——在健康和公众服务部对新兴网络安全威胁的内部响应方面，第 (1) 项要求的报告应包括以下内容：

(A) 健康和公众服务部官员发表的明确声明，表明其将负责领导和协调本部门在医疗卫生行业开展网络安全威胁的相关工作。

(B) 一份计划，说明健康和公众服务部的各相关职能部门（及分支机构）如何处置医疗卫生行业网络安全威胁，并说明为处置此类威胁，这些部门（及分支机构）如何划分人员职责、如何与其他相关部门（及分支机构）进行沟通。

##### (c) 医疗卫生行业网络安全特别工作组

(1) 一般规定——本法颁布之日起 90 日内，部长应与国家标准与技术研究院院长、国土安全部部长协商，召集医疗卫生行业利益相关方、网络安全专家以及部长认为适宜的任何联邦



机构或联邦实体，成立特别工作组，以开展下列工作：

(A) 研究分析其他行业如何实施用于处置网络安全威胁的战略和保护措施。

(B) 研究分析医疗卫生行业中，私营实体（不包括各州、部落或地方政府）在保护自身网络安全、应对网络攻击的过程中面临的障碍与挑战。

(C) 针对保护联网医疗设备和其他连接电子健康档案的软件或系统，总结相关实体和商业伙伴所面临的挑战。

(D) 向部长提供向医疗卫生行业中不同体量利益相关方进行宣传的信息，以促进它们为防范和响应影响本行业的网络安全威胁做好准备。

(E) 落实本法第 I 章规定，制定相应计划，以使联邦政府和医疗卫生行业利益相关方，能够实时共享可用于提起诉讼的网络威胁迹象信息和防护措施。

(F) 向有关国会委员会提交报告，描述特别工作组执行第 (A) 至第 (E) 目的结果和相关建议。

(2) 有效期限——根据本款规定成立的特别工作组，应于成立之日起 1 年后解散。

(3) 宣传——本款要求的特别工作组成立之日起 60 日内，健康和公众服务部部长应按第 (1) (D) 目规定，向医疗卫生行业利益相关方宣传第 (1) (D) 目所述信息。

(d) 统一医疗卫生行业安全保护方法

(1) 一般规定——健康和公众服务部部长应通过某种协同机制，协同国土安全部部长、医疗卫生行业利益相关方、国家标准与技术研究院院长以及部长认为适宜的任何联邦实体或非联邦实体，制定一套自愿采用、一致认可、行业主导的指南、最佳实践、方法论、程序和流程：

(A) 作为高效、低成本降低医疗卫生组织网络安全风险的参考资源；

(B) 支持自愿采用和实施，以强化用于处置网络安全威胁的防护措施；

(C) 符合下列法律法规的规定：

(i) 根据《国家标准与技术研究院法》第 2 (c) (15) 项（《美国法典》第 15 编第 272 (c) (15) 项）制定的标准、指南、最佳实践、方法论、程序和流程；

(ii) 根据《1996 年健康保险便利和责任法》第 264 (c) 款（《美国法典》第 42 编第 1320d-2 条注释）颁布的安全和隐私保护规定；

(iii) 《医疗信息技术促进经济和临床健康法》（公法编号 111-5，A 部分第 13 章、B 部分第 4 章）及其修正案；

(D) 并且应经常更新并应用于广大医疗卫生组织。

(2) 限制——本款中的任何规定不应被解释为，授予卫生与公共服务部部长下列权限：

(A) 为确保医疗卫生组织符合本款规定而进行审计；

(B) 或命令、指示或以授予联邦拨款、合同或采购为条件，强制医疗卫生组织遵守本款规定。

(3) 不参与者免责说明——本款中的任何规定不应被解释为，当不参与本款授权的自愿活动或不采用依本款制定的指南时，医疗卫生行业利益相关方需要承担责任。

(e) 合并正在实施的活动

对于在本法颁布前已经开展且与本条目一致的活动，健康和公众服务部部长可将其与根据本条规定执行的活动进行合并。

(f) 说明

本款中的任何规定不应被解释为，限制本法第 104 (e) 款规定的反垄断豁免或第 106 条规定的免责。

#### 第 406 条 联邦计算机安全

##### (a) 定义

在本条中：

(1) 适用系统——是指《美国法典》第 40 编第 11103 条所定义的国家安全系统，或能够访问可识别个人信息的联邦计算机系统。

(2) 适用机构——是指运营适用系统的机构。

(3) 逻辑访问控制——是指针对获取、使用信息及相关信息处理服务的具体请求，做出允许或拒绝的过程。

(4) 多因子认证——是指采用下列因子中的 2 个或 2 个以上（含 2 个）进行的认证：

(A) 用户可知的因子，如口令或身份标识码等；

(B) 提供给用户的访问设备，如密码标识设备或令牌；

(C) 用户的特定生物识别特征。

(5) 特权用户——是指能够访问系统控制、监控、或管理功能的用户。

##### (b) 检查长关于适用系统的报告

(1) 一般规定——本法颁布之日起 240 日内，各适用机构的检查长应向有管辖权的有关参议院委员会、众议院委员会提交一份报告，其中应包括根据第 (2) 项要求，从各适用机构处收集的关于该机构中联邦计算机系统的信息。

(2) 内容——各适用机构检查长依据第 (1) 项提交的报告，应包括以下内容：

(A) 针对访问适用系统，说明适用机构所采取的逻辑访问策略和最佳实践措施，包括是否符合适用的标准。

(B) 针对管理特权用户访问适用系统，说明适用机构所采取的逻辑访问控制和多因子认证，并列出清单。

(C) 针对访问适用系统，如果适用机构未采取逻辑访问控制或多因子认证，说明其原因。

(D) 说明适用实体对适用系统采取的下列信息安全管理实践：

(i) 为清点本机构适用系统中安装的软件及其证书，各适用机构采用的策略和程序；

(ii) 为监控和检测信息泄露和其他威胁，各适用机构采用的职能，包括：

(I) 数据防丢失职能；

(II) 取证和可视化职能；

(III) 或数字版权管理职能。

(iii) 说明适用机构如何运用第 (ii) 段所述职能；

(iv) 如果适用机构未采用第 (ii) 段所述职能，则应说明其原因。

(E) 说明为确保向其提供服务的实体（包括合同商）执行了第 (D) 目所述信息安全管理实践措施，适用机构所采用的策略和程序。

(3) 已有审查——本款要求的报告，可完全或部分基于对适用机构的项目或实践活动的审计、评估或报告进行编制，并且可作为其他报告（包括《美国法典》第 44 编第 3555 条要求的报告）的一部分进行提交。

(4) 涉密信息——本款要求的报告应以非涉密形式提交，但可包含涉密附件。

#### 第 407 条 禁止对美国人民金融信息进行欺诈性销售

对《美国法典》第 18 编第 1029 (h) 款做如下修订：

删除“……章，如果”及“由此”之后的所有内容，改为：“……章，如果该犯罪行为涉及由下述机构发行、拥有、管理或控制的访问设备：金融机构、账户发行者、信用卡系统成员或根据美联邦或各州、哥伦比亚特区或美国其他领土的法律组建的机构。”

---

## 二十九、国家网络安全行动计划

美国白宫

2016 年 2 月

---

采取坚定的行动，保护在当今数字世界中的美国。

自本届政府开始，总统便清晰阐明，网络安全是我们作为一个国家所面临的重要挑战之一。7年多来，他已采取全面行动应对这一挑战。在与国会合作下，2015年12月通过了《网络安全法》，这是我们在这一领域取得的另一进展。《网络安全法》提供了对加强国家网络安全而言十分必要的重要工具，特别是其使得私营公司可以更容易在彼此和政府之间分享网络威胁信息。

但总统认为必须做更多，要使公民具备保护其自己的工具，公司具备可以保卫其经营活动和信息的工具，政府具备尽职尽责保护美国人民及人民委托给我们的信息的工具。这就是为什么今天总统指挥其政府实施“国家网络安全行动计划”（CNAP）的原因。这个计划考虑了近期行动，并建立了长期的战略来加强网络空间态势感知和防护，保护隐私，维护公共安全以及经济和国家安全，并使美国人民能够更好地控制他们的数字安全。

## 1. 挑战

从购买产品到开展经营，到寻求与我们所爱的人交流，一个在线的世界从根本上重塑了我们的日常生活。但正当这个日新月异的数字时代为我们的经济、商业和我们的人民提供无尽的机会时，也带来了我们必须面对的新一代威胁。犯罪分子、恐怖分子和试图伤害我们的国家都已经意识到，在网上攻击我们往往要比面对面攻击我们容易得多。随着越来越多的敏感数据在线存储，这些攻击的后果每年都会变得越来越严重。身份盗窃如今是美国增长最快的犯罪。我们的创新者和企业家增强了我们全球的领导地位，发展了我们的经济，但随着一个个高知名度公司被黑客攻击或邻居被欺骗的新故事出现，更多的美国人开始怀疑，是否技术带来的好处正面临被其成本倾轧的风险。

总统认为，必须直面这些新的威胁，这是我们职责所在。但这需要大胆地重新评估我们在数字时代保护安全的方式。如果我们需要继续互联，我们就需要得到保护。政府、企业和个人需要站在一起来延续使美国伟大的精神。

## 2. 我们的路线

这就解释了为什么政府要在今天公布一系列近期行动计划，以提高联邦政府及全国的网络安全能力。但鉴于这个问题的复杂性和严重性，总统也在咨询政府外部的国家顶级战略、企业和技术智库，来研究和报告我们能更多地做什么，从而加强网络空间态势感知和防护，保护隐私，维护公共安全以及经济和国家安全，并使美国人民能够更好地控制他们的数字安全。需要采取勇敢的行动，保护我们数字社会的安全，保持在美国全球数字经济中的竞争力。

总统的“国家网络安全行动计划”（CNAP）是本届政府7年多坚定努力的里程碑，它建立在对网络安全趋势、威胁和入侵的教训之上。这个计划要求联邦政府立即采取新行动，并促成长期改善网络安全所需的条件，涉及联邦政府、私营部门和我们的个人生活。CNAP要点包括以下行动：

- 建立“国家网络安全促进委员会”。这个委员会将由来自政府外部的顶级战略、企业和技术智库组成，包括两党国会领袖指派的成员。委员会将为今后10年的行动提出

建议，包括加强公共-私营部门的网络安全，同时保护隐私、维护公共安全和经济及国家安全；促进新的技术解决方案的发现和制定；加强联邦、州和地方政府及私营部门在网络安全技术、政策和最佳实践的开发、推广和使用等方面的合作。

- 通过设立 31 亿美元的信息技术现代化基金，使政府信息技术变得现代化，改变政府管理网络安全的方法。这将淘汰、替换以及现代化那些难以安全和难以维护的老旧系统。同时设立一个新的岗位——联邦首席信息安全官，以推动整个政府实现上述变化。
- 使美国人民有能力保护在线账户安全，这要超越口令方式，增加额外的安全层。要将强口令与其他因子结合，如指纹或通过短信发送的单次使用验证码。通过以上措施，美国人能够使他们的账户更加安全。多因子鉴别将是“国家网络安全联盟”发起的国家网络安全意识运动的核心，旨在使消费者获取简单但可行的知识，在日益数字化的世界中保护自己。国家网络安全联盟将与领先的技术公司合作，如 Google、Facebook、DropBox 和微软公司，使数以百万计的用户更容易保护其在线账户的安全。还将与金融服务公司，如 MasterCard、Visa、PayPal 以及 Venmo 公司合作，使在线交易更安全。此外，联邦政府将采取措施保护公民与政府间在线事务中的个人数据，包括通过一项新的行动计划来推动联邦政府采用有效的身份证明方法和增强型多因子鉴别方法，系统评估联邦政府在哪些地方可以减少依赖社会安全号码作为公民标识。
- 在总统 2017 财年预算中，安排 190 多亿美元用于网络安全。这比 2016 财年整个联邦资源范围内的网络安全投入增长了 35%，对于保护今后我们国家的安全而言，这是必需的。

通过上述行动以及下面所列的其他行动，结合联邦政府其他政策努力，政府描绘了加强我们长期安全的方案，以及强化美国在开发数字世界技术方面领导地位的方案。

### 3. 国家网络安全促进委员会

40 多年来，计算机技术和互联网给美国、其人民及盟友提供了战略优势。但是如果基本的网络安全和身份问题得不到解决，美国对数字基础设施的依赖就会有成为战略性债务之源的风险。为解决这些问题，我们必须诊断和解决网络空间脆弱性的根源，而不只是处理表象。迎接这一挑战需要一个长期的国家承诺。

为了执行这一评估，总统将建立“国家网络安全促进委员会”，由来自政府外的顶级战略、企业和技术智库组成，包括由两党国会领袖指派的成员。委员会的任务是提出今后 10 年采取的具体行动建议，旨在加强网络安全态势感知，保护私营部门和各级政府的安全，保护隐私，维护公共安全和经济及国家安全，并使得美国有能力更好地控制数字安全。美国国家标准与技术研究院（NIST）将向委员会提供支持，使其能够履行这一使命。委员会将在 2016 年底前向总统报告具体的调查发现和建议，在 CNAP 基础上提供未来行动路线图，保护我们的长期在线安全。

### 4. 提升全国网络安全水平

在委员会实施这一前瞻性评估的同时，我们将持续增强整个国家的网络安全水平。

## 增强联邦政府网络安全

联邦政府已经在改进网络安全能力方面取得重大进展，但还有很多工作要做。要扩大这方面的进展，并解决联邦政府网络安全面临的长期、系统性的挑战，我们就必须重新审视政府当前的网络安全和信息技术方法，这个方法是要求每个机构建设和保护其自身的网络。这些行动建立在“网络安全跨部门优先目标”和“2015 网络安全战略和实施计划”的基础之上。

- 总统在 2017 财年预算中提出了 31 亿美元的信息技术现代化基金，这笔钱用于在后续年度采取必要措施开展全面的彻底检修。这一滚动资金将使各部门有能力对那些维护费用昂贵但功能落后、难以确保安全的 IT 基础设施、网络 and 系统进行淘汰、替换以及现代化，这是“先投入，后收益”。
- 政府设立联邦首席信息安全官职位，促进整个联邦政府中的网络安全政策制定、规划和实施。这是第一次设置一位专门的高级官员，其专注于在整个联邦范围内制定、管理和协调网络安全战略、政策和行动。
- 政府要求各部门标识最重要和面临最大风险的 IT 资产，并排列优先级，随后采取进一步的措施来切实提高其安全性。
- 国土安全部、总务管理总局及其他联邦部门将提高政府中 IT 及网络安全相关共享服务的可用性，目标是将每个部门从建设、拥有和运行自身的 IT 设施中解放出来，为它们提供更加高效、有效和安全的选项，确保各个部门在面对最复杂的威胁时不会孤军奋战。
- 国土安全部正通过扩大“爱因斯坦”项目及“连续诊断及减缓”项目，来增强联邦网络安全。总统的 2017 财年预算将支持所有联邦民事部门具备这些能力。
- 国土安全部将从整个联邦政府和私营部门招聘最优秀的网络安全人才，使联邦民事网络防御团队大幅增加到 48 支。通过渗透测试和主动捕获入侵者，同时提供事件响应和安全工程专业知识，这些团队将保护整个联邦民事政府的网络、系统和数据。
- 通过“网络安全教育国家倡议”等活动，联邦政府将加强全国范围的网络安全教育和培训，雇用更多的网络安全专家来保护联邦部门安全。作为 CNAP 的一部分，总统在网络安全人员方面的预算是 6200 万美元，包括：
  - 扩展“服务奖学金”项目，通过建立“网络部队预备役”计划，为期望获得网络安全教育并愿意进入联邦民事政府部门服务的美国人提供奖学金。
  - 开设网络安全核心课程，以确保有志于加入联邦政府的网络安全毕业生有必备的知识和技能。
  - 加强“国家网络安全学术卓越中心计划”，提高参与该计划的学术机构和学生的数量，对目前已加入的机构提供更好的支持，增加在这些机构中学习网络安全的学生数量，通过调整项目和课程来提升学生的知识。
- 总统的预算中，还将采取其他步骤，扩大网络安全从业人员：
  - 针对加入联邦政府工作的网络安全专家，强化“学生贷款免除项目”。
  - 通过“总统面向所有计划的计算机科学”项目，将网络安全作为强有力的计算机科学课程的一部分，刺激对网络安全教育的投资。

## 提升个人防护能力

所有美国人日常生活的在线隐私和安全，正在成为我们国家安全和经济的组成部分。以下新行动建立在“总统 2014 安全购买倡议”之上，旨在将加强消费者数据的安全性。

- 总统呼吁美国人要超越口令，当登录在线账户时，要利用多因子身份鉴别方式。私人公司、非营利组织以及联邦政府正共同努力，通过一场新的意识宣传运动，重点是广泛采用多因子身份鉴别，帮助更多的美国人实现在线安全。建立在“一停二想再连接”运动及“网络空间可信身份国家战略”相关工作的基础上，国家网络安全联盟将与领先的技术公司和民用领域合作，使数以百万的用户更容易保护自己在线账户的安全。这将支持范围更广的工作，以提升公众对个人在网络安全中角色的认识。
- 在面向公民的联邦政府数字服务中，联邦政府正在加速采用强大的多因子身份鉴别和身份证明方式。总务管理局将建立一项新计划，当美国人与联邦政府服务打交道时，将更好地保护数据和个人信息安全，包括税收数据和福利信息。
- 政府正在系统性地评估，联邦政府可以在哪些方面减少依赖社会安全号码作为公民的标识符。
- 联邦贸易委员会最近重新启动了 IdentityTheft.Gov 网站，可在以下方面提供一站式资源服务：受害者报告身份信息被窃，创建个人信息恢复计划，打印预填写的拟发送给征信机构、企业和收账员的信函和表格。
- 小企业管理局（SBA）与联邦贸易委员会、国家标准与技术研究院（NIST）和能源部将通过 68 个 SBA 小企业管理局地方办公室、9 个 NIST 制造业扩展合作中心以及国内其他的区域性网络，为 140 万小企业和小企业利益相关者提供网络安全培训。
- 政府在“总统安全购买倡议”中，正在公布新的里程碑，以确保金融交易安全。迄今为止，联邦政府已提供超过 250 万的更安全的芯片加 PIN 码支付卡，并在财政部管理的所有读卡器上采用了这项新技术。通过政府和私营部门领导，美国已经发行了比世界上任何其他国家更安全的芯片卡。

## 加强关键基础设施安全和韧性

美国的国家和经济安全取决于国家的关键基础设施的可靠运行。关键基础设施的所有者与运营者的持续合作将提高网络安全并增强国家的抗打击能力。这项工作建立在总统此前发布的 2013 年关键基础设施行政令和 2015 年发布的信息共享行政令基础之上。

- 国土安全部、商务部和能源部正在贡献资源和能力，以建立“国家网络安全韧性中心”。在这里，公司和行业组织可以在一个封闭的环境中测试系统的安全性，如测试一个复制的电网遭受网络攻击的情况。
- 国土安全部将成倍增加网络安全顾问，以协助私营部门开展现场的定制化网络安全评估，实现最佳实践措施。
- 国土安全部正在与 UL 和其他行业伙伴制定“网络安全保障计划”，以测试和认证物联网中的联网设备，无论它们是冰箱或医用输液泵，以使用户购买新的产品时，可以确保其已获认证，符合安全标准。
- 国家标准与技术研究院正在为进一步发展其“网络安全框架”征求反馈意见。该框架旨在提高关键基础设施网络安全。这项工作已在全国各地及全世界开展两年。



- 昨天，商务部长普里茨克为新的国家网络安全卓越中心剪彩，这是公共-私营合作开展研发的一种伙伴关系，将使得工业界和政府可以共同工作来开发和部署面对高优先级网络安全挑战的技术解决方案，并与更广泛的团体共享研究结论。
- 政府正在向大型医疗保险和健康领域的利益相关者发起号召，以帮助它们采取新的重大步骤来强化数据管理措施，确保消费者可以确信，他们敏感的健康数据将是安全、可靠的，并对于指导临床决策是可用的。

### 安全技术

即使今天努力改善我们的防御态势，我们也要知道国家必须大举投资未来的科学、技术、工具和基础设施，确保它们在工程化时已将持续性的安全置入其中。

- 今天，政府正在发布《2016 年联邦网络安全研发战略计划》。这是《2014 年网络安全增强法》中提出的任务。这个战略规划描绘了国家的战略研发目标，以促进在有效性、高效性科学证据驱动下的网络安全技术发展。
- 此外，政府将与 Linux 基金会的“核心基础设施倡议”等合作，资助并强化常用的互联网工具的安全，如开源软件、协议和标准。正如我们的道路和桥梁需要定期维修和保养，技术这个桥梁也是如此，正是它使得信息在超高速公路流动。

## 5. 威慑、劝阻和终止网络空间恶意活动

更好地保护我们自己的数字基础设施只是解决方案的一部分。即使正在采取措施威慑和阻止恶意活动，我们也必须带领国际社会，采用负责任的国家行为原则。我们不能单独追求这些目标，而必须与我们的盟国和世界各地的伙伴共同追求这些目标。

- 2015 年，G20 成员国与美国就重要规范达成一致，包括国际法在网络空间的适用性，各国政府不应支持出于商业目的利用网络盗取知识产权的行为，欢迎联合国政府专家组发布相关报告、加强国际合作，防止对民用基础设施的攻击，支持计算应急小组提供重建和容灾服务。政府试图通过进一步的双边或多边承诺，建立信任措施实施这些准则。
- 美国司法部，包括联邦调查局，将增加 23% 以上的网络安全相关活动经费，提高其定位、阻止和逮捕网络恶意行为者的能力。
- 美国网络战司令部正在建设一个有 133 支小分队的网络部队，包括 6 200 位军人、文职、合同商保障人员等。该部队将于 2018 年全面运作，目前正在通过各类网络行动来支持美国政府的目标。

## 6. 改进网络空间事件响应

即使专注于预防和阻止恶意网络活动，当事件发生时，我们也必须保持韧性。在过去一年，从犯罪活动到网络间谍活动，国家遇到了各种入侵活动。通过吸取过去事件的教训，我们可以改善未来网络安全事件管理，提高国家的网络韧性。

- 今年春天，政府将公开发布国家网络事件协调政策以及配套的网络事件严重性评估方法，使得政府机构和私营部门可以有效沟通，进行适宜和一致的响应。

## 7. 保护个人隐私

与上述信息技术和网络安全努力相配套，政府已经发起了一项开创性的工作，以提高整个联邦政府机构保护个人隐私及其信息的能力。自我们的国家建立以来，隐私就一直是核心，在当今的数字化时代保护隐私比以往更加重要。

- 今天，总统签署了行政命令，要创建一个常设的联邦隐私委员会。该委员会将汇集来自政府各部门的隐私官员，以有助于确保更具战略性和更全面的联邦隐私准则的实施。与网络安全类似，在我们国家拥抱新技术、促进创新、获益于大数据和抵御不断变化的威胁的同时，隐私必须得到有效和持续的关注。

## 8. 网络安全投入

为了实现这些彻底的变化，联邦政府需要在网络安全领域投入更多资源。这就是为什么 2017 财年预算在网络安全方面超过 190 亿美元（比 2016 财年增加了 35%）的原因。这些资源将使各部门得以提高他们的网络安全水平，帮助私营部门的组织和个人更好地保护自己、瓦解和阻止对手的活动，以及更有效地响应事件。

---

## 三十、第 41 号总统政策令：美国网络事件 协调

美国白宫

2016 年 7 月 26 日

---

网络技术的出现推动了科技创新、知识积累、言论自由和国民经济的繁荣发展。然而，支撑这些发展的基础设施极易受到各种攻击，包括恶意活动、功能故障、人为错误和自然灾害等，使得国家和人民面临巨大风险。当今生活中，网络事件是一个残酷的现实，并且重大网络事件频频发生，严重影响着国内、国外的美国公共-私营基础设施。

凭借充分的准备，美国得以有效管理大量的威胁和危险。为了保护信息和通信基础设施安全，联邦执法部门和网络防御部门每天管理、响应和调查大量网络事件。保护国家免受恶意网络活动侵害，管理网络事件及其后果，对私营部门和政府机构都至关重要。网络空间的本质要求个人、组织和政府在网络事件响应方面共管共治。而且，对网络事件的有效响应将有助于建立开放、合作、安全和可靠的信息和通信基础设施，进而推动商贸发展、加强国家安全、促进言论自由、强化个人隐私和安全保护。

尽管现有政策可以处理大部分网络事件，但是某些网络事件可能对单个实体、国家安全，甚至更广泛的经济发展产生重大影响，因此，需要制定统一的响应措施。这些重大网络事件的处理需要联邦政府内部的统一协调部署，尤其是需要公共-私营部门的紧密协作。

## 1. 范围

本总统政策令（PPD）给出了基本原则，管理联邦政府对网络事件的响应行动，不论这些网络事件是涉及政府，还是涉及私营部门实体。针对重大网络事件，本令明确了牵头联邦机构，并为协调多个联邦政府部门的响应行动制定了一个框架。同时，本令也要求司法部和国土安全部保持最新的公开联系方式，帮助受网络事件影响的实体向适宜的监管部门报送网络事件。

## 2. 定义

（1）网络事件：是指在计算机网络中发生或通过其实施的，对计算机、信息或通信系统及网络控制的物理或虚拟基础设施，以及其上存储的信息的完整性、保密性或可用性已实际产生或即将产生危害的事件。对于本 PPD 而言，网络事件还可能包括在信息系统、系统安全程序、内部控制措施或实施方案中存在的脆弱性，威胁源正是利用了这些脆弱性。

（2）重大网络事件：是指可能对美国的国家安全、外交关系或经济发展，以及美国人民的公众信心、公民自由、公共健康与安全造成严重危害的网络事件或一组相关的网络事件。

## 3. 事件响应的指导原则

在实施网络事件响应行动时，联邦政府应遵循以下五项原则。

（1）责任共担：在保护国家免受恶意网络活动侵害和管理网络事件及其后果方面，个人、私营部门和政府机构关键利益一致、角色互补、责任共担。

（2）基于风险的响应：联邦政府应基于对单个实体、国家安全、外交关系、经济发展、公众信心、公民自由、公众健康与安全的风险评估，确定响应行动和资源提供。

（3）尊重受害实体：在通知其他受害私营部门实体和公众时，联邦政府将在法律允许范围

内尽可能保护受害实体，保护事件细节信息、个人隐私、公民自由以及敏感私营部门信息。如果出于维护联邦政府重要利益的考虑，需要就某一网络事件发布公开声明，联邦政府将尽最大可能与受害实体协商响应方式。

(4) 政府机构协调一致：在应对网络事件时，不同政府实体扮演着不同角色，具有不同的责任、权限和职能。为了取得最佳应对效果，必须对其进行统一协调。无论哪个部门最先发现网络事件，都应快速通知其他相关联邦机构，以形成统一的联邦响应行动，确保由适当联邦机构联合响应这一网络事件。州、地方、部落和领地（SLTT）政府也具有响应网络事件的责任、权限、职能和资源。因此，在实施网络事件响应行动时，联邦政府必须做好与州、地方、部落和领地（SLTT）政府合作的准备。考虑到互联网和通信基础设施跨越国界的性质，适当时，美国还应与国际合作伙伴协作，共同应对网络事件。

(5) 利于恢复与复原：联邦响应活动应有利于网络事件受害实体的恢复与复原，同时平衡考虑事件调查和国家安全需求、公众健康与安全以及尽快恢复正常业务的需要。

## 4. 并行工作方向

在响应任何网络事件时，联邦机构都应采取三个并行工作方向：威胁响应、资产响应、情报支持及相关活动。另外，当联邦机构是受害实体时，该机构应采取第四个并行工作方向，以管控网络事件对其运行、客户和员工的影响。

(1) 威胁响应行动：包括以下活动：在受害实体现场实施适当的执法和国家安全调查；取证和情报收集；溯源；事件关联分析；确定其他受害实体；研判对威胁进行追踪和阻断的机会；制定和执行系列活动以缓解当前威胁；推动与资产响应进行信息共享和行动协调。

(2) 资产响应行动：包括以下活动：为受害实体提供技术帮助，以保护其资产、减轻脆弱性和降低网络事件的影响；确定其他可能处于风险中的实体，并评估其受到相同或类似脆弱性影响的风险；评估行业或区域潜在风险，包括潜在的连锁影响，并制定系列活动减轻这些风险；推动与威胁响应进行信息共享和行动协调；提供如何更好地使用联邦资源和职能以及及时有效进行恢复的指南。

威胁和资产响应方将共享责任和活动，包括：与受害实体沟通，以理解网络事件的基本特征；为受害实体提供指南，说明可用的联邦资源和职能；立即通过适当的渠道，将在响应事件过程中获得的情报和信息进行分发；推动与其他联邦政府实体进行信息共享和行动协调。

(3) 情报支持及相关行动：将促进以下事项：威胁态势感知的建立和相关情报的共享；威胁趋势和事件的综合分析；知识差距的确定；对敌对威胁进行削弱或打击的能力。

(4) 受影响的联邦机构应采取各种措施：管理网络事件带来的影响，包括：维持业务或运行的连续性；应对财务方面的负面影响；隐私保护；管理责任风险；遵循法律和监管要求（包括披露和通知）；与雇员或其他受影响的个人进行沟通；处理外部事务（如媒体和国会质询等）。受影响联邦机构对上述行动负有主要责任。

当网络事件仅影响单个私营实体时，联邦政府通常不会作为主体采取第四项行动，但会根据上述原则，与受害实体协商，实时关注受害实体的响应行动。与关键基础设施对口的相关政府部门（SSA）将协调联邦政府的有关工作，以了解在业务和运行方面，网络事件可能对私营部门关键基础设施产生的影响。

## 5. 针对重大网络事件的联邦政府响应协调框架

为了有效响应重大网络事件，联邦政府将从以下三个方面协调响应行动。

### A. 国家政策协调

网络响应小组（CRG）支撑国家安全委员会（NSC）的代表委员会和主管委员会，并通过总统国土安全和反恐助理（APHSCT）对国家安全委员会（由总统直接领导）负责。同时，应针对影响美国或美国国际利益的重大网络事件，协调美国政府相关政策的制定与实施。

### B. 国家行动协调

#### a. 各机构的增强性协调流程

为了应对重大网络事件响应需求超过联邦机构现有能力的局面，每个参与网络响应小组（包括关键基础设施对口的相关政府部门（SSA））事务的联邦机构，都应制定并遵循本令附录中定义的增强性协调流程。

#### b. 网络统一协调小组（Cyber UCG）

在响应重大网络事件时，网络统一协调小组是在联邦机构间协调的主要方式，需要时，也是把私营部门合作伙伴整合到事件响应过程中的主要方式。网络统一协调小组的成立应符合以下条件之一：受国家安全委员会代表委员会和主管委员会或网络响应小组的指示；当两个（含）以上参与网络响应小组（包括关键基础设施对口的相关政府部门（SSA））事务的联邦机构提出要求时；如果重大网络事件将影响关键基础设施所有者和运营者，且国土安全部部长确定此类事件可能对公共健康或安全、经济安全或国家安全，造成区域性或国家级的灾难性影响。

网络统一协调小组通常由负责威胁响应、资产响应和情报支持的联邦领导机构组成，但当网络事件影响或可能影响某一关键基础设施行业时，也会包括关键基础设施对口的相关政府部门（SSA）。另外，根据个别重大网络事件范围、性质和实际情况的不同，网络统一协调小组也可能包括其他联邦机构、SLTT（州、地方、部落和领地）政府、非政府组织、国际合作伙伴或私营部门等。

网络统一协调小组成立后，成员联邦机构应履行相应的责任，调配适当的高级行政官员、工作班子和资源。网络统一协调小组旨在形成合力而并不是改变机构权限或领导、监管或指挥的责任。联邦部、局负责管理各自机构的资产，除非根据适用的法律授权，如《1932年经济法案》（《美国法典》第31编第1535条），双方机构负责人或其指定代表达成一致放弃资产控制权。

#### c. 联邦领导机构

在协调重大网络事件响应的过程中，为了确保网络统一协调小组取得最大成效，以下机构将作为特定行动的领导机构：

（1）鉴于重大网络事件通常至少涉及国家、州一级的行为体，或在某种程度上关系到国家安全，所以司法部应作为威胁响应行动的联邦领导机构，通过联邦调查局和国家网络调查联合特遣队开展工作。

（2）国土安全部应作为资产响应行动的联邦领导机构，通过国家网络安全和通信整合中心开展工作。

（3）国家情报总监办公室应作为情报支持和相关行动的联邦领导机构，通过网络威胁情报整合中心开展工作。

通过利用联邦政府的资源和职能，联邦领导机构对以下行动负责：

- 协调由多家机构参与的威胁或资产响应行动，形成合力，包括协调任何可以为事件提供专业技术支持的机构和行业主管部门。
- 适当时，确保联邦机构的响应行动与其他网络统一协调小组参与者和受害实体协调一致。
- 如果需要进行评估，确定适当的响应和恢复所必需的任何进一步的联邦政府资源或行动，向网络响应小组提出建议。
- 并且适当时，通过网络统一协调小组，与受害实体合作开展威胁响应、资产响应和受害实体响应行动。

### C. 现场协调

负责资产响应或威胁响应的联邦领导机构现场代表应确保，能够在联邦领导机构之间以及与受害实体之间，有效协调其各自的响应行动。

## 6. 一致的公共联络

国土安全部和司法部应提供一份公开资料，并保持更新，说明发生网络事件时个人和私营组织如何联系相关联邦机构。

## 7. 与现有政策的关系

本令任何内容不应改变、替代或限制，联邦机构根据合法授权、其他总统指南和总统令履行其职责的权限。总体而言，本令依靠并推动现有政策的实施，并说明了美国网络事件响应框架如何与现有政策相互协调工作。尤其是，本令建立在 2011 年 3 月 30 日发布的总统政策令《国家战备》（PPD-8）基础之上，并对其进行了补充。通过整合网络 and 传统战备措施，国家将做好管理网络和物理事件的准备。

注：本令中，关于国家网络响应协调小组的文字替代了第 54 号国家安全总统令/第 23 号国土安全总统令（NSPD-54/HSPD-23）的第 13 段。

## 附录 重大网络事件联邦政府协调框架

### 1. 范围

本文是“美国网络事件协调”（PPD-41）的附录，详细描述了重大网络事件联邦政府协调框架以及部分实施任务。

### 2. 协调框架

#### A. 国家政策协调

网络响应小组应由总统特别助理和网络安全协调员（主席）或同级别官员领导，并应定期或需要时，根据总统国土安全和反恐助理、副国家安全顾问的要求召开会议。适当时，根据联

邦部和局（包括相关网络中心）角色、责任和专业知识的，或者某一（组）特定网络事件的需要，应邀请他们参与网络响应小组相关事务。一般来讲，网络响应小组应包括来自以下部门的高层官员代表：国务院、财政部、国防部、司法部、商务部、能源部、国土安全部、国家保护和计划理事会、美国特勤处、参谋长联席会议、国家情报总监办公室、联邦调查局、国家网络调查联合特遣队、中央情报局和国家安全局。如果评估后，网络响应小组主席认为联邦通信委员会的参与是形势所必需，且联邦通信委员会确定其参与活动符合法律权限和法定义务，应邀请联邦通信委员会参与网络响应小组的相关事务。

网络响应小组应：

- (i) 针对重大网络事件响应，协调联邦政府政策、战略和程序的制定和实施。
- (ii) 从联邦的各个网络中心和机构，接收关于重大网络事件及其解决或响应措施的定期更新信息。
- (iii) 解决下属机构上报信息的问题，如网络统一协调小组。
- (iv) 当重大网络事件需要跨部门的响应行动时，与反恐安全小组和国内恢复小组合作开展工作。
- (v) 根据 2009 年 2 月 13 日颁布的总统政策令“国家安全理事会系统组织”（PPD-1）或其后继文件，当需要高层指导时，向代表委员会提供关于确定重大网络事件及可选响应方案的建议。
- (vi) 重大网络事件响应行动应考虑公开信息的政策倾向问题，需要时，应协调制定一份与此有关的通信战略。

## **B.国家行动协调**

为了促进重大网络事件的统一响应行动，网络统一协调小组应：

- (i) 根据本令第 III 部分“事件响应的基本指导原则”的要求，协调网络事件响应行动。
- (ii) 确保所有相关联邦机构都参与事件响应行动，包括关键基础设施对口的相关政府部门（SSA）。
- (iii) 针对事件响应和快速恢复，协调所需任务、优先事项和规划工作等的制定和执行。
- (iv) 针对事件响应和快速恢复行动相关信息和情报，推动其在网络统一协调小组参与单位内快速和恰当的共享。
- (v.) 为事件受害方和利益相关方，适当时包括公众，提供协调一致的、准确的和合适的通信方式。
- (vi) 针对包括网络和物理影响的事件，在“国家响应框架”（根据 2011 年 3 月 30 日颁布的总统政策令“国家准备”（PPD-8）所制定）下，与联邦领导机构或任何管理物理影响的统一协调小组建立一个联合统一协调小组。

如果重大网络事件影响或可能影响某一关键基础设施行业，则其统一协调小组成员应包括关键基础设施对口的相关政府部门（SSA）。根据总统政策令“关键基础设施安全与韧性”（PPD-21），关键基础设施行业对口政府部门包括国土安全部（包括化学、商业设施、通信、关键生产企业、大坝、应急服务、政府设施、信息技术、核反应堆、材料、废品和运输系统）、国防部（国防工业基地）、能源部（能源）、财政部（金融服务）、农业部（食物与农业）、健康与公共服务部（医疗保健与公共卫生、食物与农业）、总务管理局（政府设施）、交通部（运输系统）、环境保护局（供水和废水系统）。

网络统一协调小组的运行应符合有关信息的保护需求，如情报与执法来源、方法、运行和



调查，个人隐私以及敏感私营部门信息等。

当不再需要威胁响应和资产响应的增强性协调流程时，或者不再需要多家联邦机构的权限、职能或资源来管理联邦事件响应的遗留问题时，网络统一协调小组应解散。

### 3. 联邦政府对影响联邦网络事件的响应

本令任何内容不会改变某一机构对下列要求的遵循义务：遵循 2014 年《联邦信息安全现代化法》（FISMA）及管理办公室指南的要求，主要是指与其定义的“事件”、“违反”或“重大事件”相关的要求。联邦机构应根据管理和预算办公室指南，确定一个事件是否应定义为“重大事件”。如果一个网络事件符合“重大事件”标准，则这个事件也是本令定义的“重大网络事件”，并应根据本令要求进行管理。

#### A. 民用联邦网络

管理和预算办公室主任负责联邦机构信息安全政策与实践的监管。国土安全部部长通过与管理和预算办公室主任协商，负责管理联邦机构信息安全政策和实践，以及运行联邦信息安全事件中心。国家标准与技术研究院负责制定联邦信息系统的标准和指南，供联邦机构使用。

联邦机构应根据本令和适用的政策及程序，响应重大网络事件，包括根据 US-CERT（美国联邦美国计算机应急准备小组）的事件通知指南的要求，向国土安全部进行报告。

当重大网络事件仅影响单一联邦机构的运行活动时，受害机构应承担受害资产响应行动的主要职责，并负责服务及相关网络、系统与应用的恢复以及拥有重启受害系统的决定权。国土安全部和其他联邦机构应提供相应的帮助。

当重大网络事件影响多家联邦机构，或影响公共服务的完整性、保密性或可用性时，受害系统所属联邦机构具有重启系统的决定权。但是，管理和预算办公室和负责威胁响应与资产响应的联邦领导机构，应提供及时、统一的书面建议以及适当的注意事项和应用条件，帮助该联邦机构进行正确的决策。

#### B. 国防部信息网络

针对影响国防部信息网络的网络事件，国防部部长应负责管理威胁响应和资产响应，包括恢复行动。必要时，可以寻求其他联邦机构的帮助。

#### C. 情报共同体网络

针对情报共同体信息环境的综合防御，国家情报总监应通过情报共同体安全协调中心，负责管理相应的威胁响应和资产响应。必要时，可与情报共同体合作伙伴协商，并得到其他联邦机构的帮助。

### 4. 实施与评估

为实施本令，联邦机构应采取以下行动。

#### A. 宪章

本令颁布之日起 90 天内，国家安全委员会工作班子应更新网络响应小组的宪章，要体现并支持根据本令制定的政策，并通过总统国土安全和反恐助理将更新后的宪章提交给总统。

#### B. 增强性协调流程

每个参与网络响应小组的联邦机构（包括关键基础设施对口的相关政府部门（SSA））都应确保在网络事件响应过程中具有独立履行相应义务的能力。本令颁布之日起 90 天内，针对重大网络事件响应要求可能会超过本机构独立能力的情况，每个机构都应建立增强性协调流

程。尽管对重大网络事件响应要求超过了本机构在正常运行条件下的协调能力，当增强性协调流程启动时，机构也要有专责领导、支撑性人员、辅助设施（物理和通信）和内部流程。

本令颁布之日起 90 天内，根据需要，并在符合本令的前提下，关键基础设施对口的相关政府部门（SSA）应与各关键基础设施部门协商，制定和更新本行业的增强性协调流程，支持对重大网络事件的响应。

在重大网络事件发生时，增强性协调流程应：确定与其他联邦机构的通信方式，包括相关的联络人，还要有将增强性协调流程已激活或启用的情况通知网络响应小组的适宜方式；重点关注与有效的事件协调相一致的内部通信和决策过程；并列明用于维持这些增强性协调流程的处理过程。

另外，每个联邦机构的增强性协调流程都应确定，在符合本令要求的条件下，本机构用于协调网络事件响应的流程和现有职能。增强性协调流程应确定一个经过培训的高层行政领导，监管本机构参与网络统一响应小组的相关事务。针对总统政策令“关键基础设施的安全与韧性”（PPD-21）定义的不同关键基础设施行业，每个关键基础设施对口的相关政府部门（SSA）都应有一个经过培训的高层行政领导。

本令颁布之日起 120 天内，关键基础设施对口的相关政府部门（SSA）应协调关键基础设施所有者和运营者，同步更新各基础设施部门的规划，与保持与本令一致。

#### **C.培训**

本令颁布之日起 150 天内，联邦应急管理局应对现有统一协调培训进行必要的更新，以吸收本令的基本原则。

本令颁布之日起 150 天内，各联邦机构应更新其各自的网络事件协调培训，以吸收本令的基本原则。

为了管理和响应重大网络事件，各联邦机构应在“国家事件管理系统和统一协调”中，明确和维持一批合格且经过培训的核心人员。他们将提供必要的专业知识，以支撑网络统一协调小组的任务和决策。

#### **D.演习**

本令颁布之日起 180 天内，各联邦机构应将本令的基本原则纳入网络事件响应演习中，包括“国家演习计划”中的相关演习。演习应按照必要的频率定期举行，以确保各联邦机构已为执行本令要求的计划和流程做好了准备。适当时，演习应考虑端到端信息共享流程的有效性。

#### **E.网络统一协调小组事后总结**

每个网络统一协调小组解散后，主席都应总结该网络统一协调小组在重大网络事件发生时所采取的响应行动，并在总结的基础上，30 天内形成报告，提交给网络响应小组。根据该报告，各联邦机构应对其负责的计划或流程进行适宜或必要的修改。

#### **F.国家网络事件响应计划**

本令颁布之日起 180 天内，经与关键基础设施对口的相关政府部门（SSA）相协调，国土安全部和司法部应通过总统国土安全和反恐助理及管理 and 预算办公室主任，向总统提交网络统一协调小组的运行纲要。该运行纲要应符合本令规定的原则、政策和协调框架，进一步描述网络统一协调小组和联邦协调框架的现场部门如何在实践中进行协作，以响应重大网络事件，包括与负责管理事件之物理影响的联邦机构相协调的机制（在该事件同时会产生物理和网络影响的情况下）以及适当时在响应行动中整合私营行业实体的机制。必要时，国土安全部部长应在

《2015 年网络安全法》205 条要求的网络事件附件中，整合或参考该运行纲要。

本令颁布之日起 180 天内，国土安全部部长应与司法部长、国防部部长和各关键基础设施对口的相关政府部门（SSA）相协商，并通过总统国土安全和反恐助理、管理和预算办公室主任，向总统提交应对网络安全风险的国家网络事件响应计划。该计划应符合本令规定的基本原则、政策和协调框架。国土安全部部长应确保该计划符合《2014 年国家网络安全保护法》第 7 条的要求。该计划的制定应与 SLTT（州、地方、部落和领地）政府、各关键基础设施部门协调委员会、信息共享与分析组织、关键基础设施所有者和运营者以及其他有关实体和个人进行协商。该计划还应该考虑，这些利益相关方如何与各联邦机构进行协调，以对影响关键基础设施的网络事件进行处置、响应并从中恢复。

---

## 三十一、国家网络事件响应计划

美国国土安全部

2016 年 12 月

---

## 1. 执行摘要

网络技术已触及全球每个角落和人类生活的各个方面，驱动创新、培育自由并促进经济繁荣。然而，这些为人类带来裨益的技术也给恶意和有害的网络活动提供了新机会。为了应对网络技术带来的风险，政府发布了第 41 号总统政策令“美国网络事件协调政策”（PPD-41），该政策令提出了联邦政府对任何网络事件进行响应的原则，无论此类事件是影响政府还是私营部门实体。

PPD-41 认为网络事件发生的频率正不断增加，这种趋势在短时间内不会扭转。针对可能影响美国国家安全、外交、经济、公众信心、公民自由、公众健康和安全的一系列重要事件，需要统一规划、统一协调并开展响应演练，以减少网络事件对国家、关键基础设施和公民生活的威胁。

本“国家网络事件响应计划”（NCIRP）根据 PPD-41 进行制定，并参照国家战备体系定义了各方角色、责任、能力和协调结构，旨在支持国家在重大网络安全事件中的响应和恢复。NCIRP 并非战术或操作计划，而是一个应对网络事件的主要战略框架，使利益相关方可以了解联邦政府各部、局及其他国家层面合作伙伴如何为响应活动提供资源支持。在政府和私营部门合作伙伴密切协调下，NCIRP 根据 PPD-41 解释了并行工作线的含义，即联邦政府如何组织其行动，以管理重大网络事件影响。并行工作线包括威胁响应、资产响应、情报支持及受影响实体的响应，旨在管理事件对业务、客户和员工产生的影响。网络统一协调小组（UCG）内的各项行动及有关联邦领导机构如下所述：

- 司法部是负责重大网络事件威胁响应的领导机构，通过联邦调查局和国家网络调查联合特遣队开展工作。威胁响应包括：在受影响实体的现场开展执法和国家安全调查；收集证据和情报；溯源；对相关事件进行关联；识别其他受影响实体；研判威胁动机及对威胁的阻断机会；制定并执行可减轻威胁的行动方案；与资产响应活动进行信息共享和运行协调。
- 国土安全部是负责重大网络事件资产响应的领导机构，通过国家网络安全和通信整合中心开展工作。资产响应包括：向受影响实体提供技术援助以保护其资产；降低脆弱性；减少网络安全事件影响；识别可能面临风险的其他实体；评估事件对各关键基础设施部门或区域的潜在风险，包括潜在的级联效应；制定可减轻威胁的行动方案；与威胁响应活动进行信息共享和运行协调；提供指南，说明如何及时利用联邦的资源 and 能力来加快事件恢复。
- 威胁响应者和资产响应者将共同承担某些责任和行动，包括与受影响实体沟通，了解网络事件性质，向受影响实体提供可用联邦资源和能力的指南，及时将响应中的情报和信息通过适当渠道传播，促进与其他联邦政府实体之间的信息共享和运行协调。
- 国家情报总监办公室是负责重大网络事件情报支持的牵头协调机构，通过网络威胁情报整合中心开展工作。情报支持和相关行动包括：为联邦资产和受威胁机构提供支持；推动建立威胁感知和相关情报共享能力；对威胁趋势和事件进行整合分析；识别知识差距；降低或减轻事件威胁的能力。
- 受影响联邦机构应进行尽一切努力来管理网络事件带来的影响，包括维持业务或运行

的连续性、处理不利的金融影响、保护隐私、管理责任风险、遵守法律法规要求（包括披露和通知）、与员工或其他受影响人员沟通、处理外部事务（如媒体和国会调查），并对这一系列活动负主要责任。

- 联邦政府通常不会在受影响的私营实体的响应中发挥作用，但将关注受影响实体的响应行动，遵循上述原则与受影响实体相协调。各关键基础设施对口的相关政府部门（SSA）将协调联邦政府的有关工作，了解网络事件对私营部门关键基础设施在业务或运行方面的潜在影响。

NCIRP 建立在一系列并行工作基础之上，履行了国家对加强网络技术和基础设施的安全性和韧性的承诺。该计划为各利益相关方制定其机构、部门和组织的特定响应计划提供了指南。同时，该计划会根据需要进行持续更新，以反映技术发展带来的机遇和挑战，确保该计划能充分应对不断变化的威胁环境。

## 2. 简介

根据《2014 年国家网络安全保护法》（NCPA）<sup>①</sup>的规定（该法后来在《国土安全法》<sup>②</sup>中做了修订），经与有关实体和个人相协调，国土安全部（DHS）要开发并定期更新、维护和演练可调整的 NCIRP，以应对关键基础设施的网络安全风险。PPD-41 及相关附录<sup>③</sup>提出了联邦政府对任何网络事件进行响应的原则，建立了一个协调响应重大网络事件的架构，并要求 DHS 制定 NCIRP，以应对关键基础设施的网络安全风险。作为国家战备体系的一部分，NCIRP 建立了一个战略框架并提出了一个举国方法<sup>④</sup>来应对网络事件，该方法十分依赖与公共-私营合作伙伴的关系。

- NCIRP 的目的和组织：为应对影响关键基础设施的重大网络事件，NCIRP 提出了一个举国方法，为实施响应行动及同利益相关方协调提供了指南。NCIRP 为国家、基础设施部门和个体组织的网络运行计划制定了原则和战略框架。
- 目标受众：NCIRP 的目标受众是美国的机构，也可用于增强国际合作伙伴对美国网络事件协调的理解。这一举国概念聚焦于各类利益相关方的工作，并推动这些利益相关方全面参与事件响应活动。这些利益相关方包括私营部门、非营利组织（包括关键基础设施的私营和公共所有者、运营者）、州、地方、部落、领地（SLTT）政府以及联邦政府等。仅仅依靠政府资源不足以应对重大网络事件，每个合作伙伴都应共同参与并形成合力来应对重大网络事件。

---

① 公法 113-282，2014 年 12 月 18 日。

② 《美国法典》第 6 编第 149 节。

③ PPD-41 《美国网络事件协调》。<https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination, <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>.

④ 举国方法还包含很多新的和现有的公共-私营合作模式，尽最大可能成为对关键基础设施网络安全威胁和风险进行管理的工作平台。

### 3. 范围

网络事件响应是与信息和通信技术（ICT）、运行技术有关的工作和系统的重要组成部分。有效地实施事件响应是一项复杂任务，需要大量的规划和资源来建立完善的事件响应能力。

NCIRP 是联邦与 SLTT 政府、私营部门、国际合作伙伴进行运行协调的战略框架。NCIRP 根据 PPD-41、国家战备体系和国家事件管理体系（NIMS）<sup>①</sup>的指导原则进行制定。这是一个针对网络事件如何进行国家规划、准备和响应的战略框架，建立了用来协调更广泛团体的响应活动的体系结构，以遵循美国法律和政策，响应重大网络安全事件。政策文件列表参见附录 A（政策文件和法规）。在 NCIRP 制定过程中，还参考了国家标准与技术研究院（NIST）制定的“增强关键基础设施网络安全框架”<sup>②</sup>。

NCIRP 并非战术或操作计划。然而，它为利益相关方制定本机构、本关键基础设施部门和本组织的专门运行计划提供了主要的战略框架。NCIRP 将帮助受事件影响的机构了解联邦各部、局和其他国家层面合作伙伴如何为影响网络事件提供资源支持。同时，NCIRP 也可作为国家网络运行手册和各关键基础设施部门运行协调计划的基础，各实体在制定其自己的计划时也可参考 NCIRP。无论何时，事件响应行动应遵循相关法律和政策。

#### 指导原则

NCIRP 根据 PPD-41 的指导原则进行制定，这些原则包括：

- 责任共担：在保护国家免受恶意网络活动侵害和管理网络事件及其后果方面，个人、私营部门和政府机构关键利益一致、角色互补、责任共担。
- 基于风险的响应：联邦政府应基于对单个实体、国家安全、外交关系、经济发展、公众信心、公民自由、公众健康与安全的风险评估，确定响应行动和资源提供。
- 尊重受害实体：在通知其他受害私营部门实体和公众时，联邦政府将在法律允许范围内尽可能保护受害实体，保护事件细节信息、个人隐私、公民自由以及敏感私营部门信息。如果出于维护联邦政府重要利益的考虑，需要就某一网络事件发布公开声明，联邦政府将尽最大可能与受害实体协商响应方式。
- 政府机构协调一致：在应对网络事件时，不同政府实体扮演着不同角色，具有不同的责任、权限和职能。为了取得最佳应对效果，必须对其进行统一协调。无论哪个部门最先发现网络事件，都应快速通知其他相关联邦机构，以形成统一的联邦响应行动，确保由适当联邦机构联合响应这一网络事件。州、地方、部落和领地（SLTT）政府也具有响应网络事件的责任、权限、职能和资源。因此，在实施网络事件响应行动时，联邦政府必须做好与州、地方、部落和领地（SLTT）政府合作的准备。考虑到互联网和通信基础设施跨越国界的性质，适当时，美国还应与国际合作伙伴协作，共同应对网络事件。
- 利于恢复与复原：联邦响应活动应有助于网络事件受害实体的恢复与复原，同时平衡

<sup>①</sup> <http://www.fema.gov/national-incident-management-system>。

<sup>②</sup> 美国国家标准与技术研究院（NIST），2014 年 2 月 12 日，<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>。

考虑事件调查和国家安全需求、公众健康与安全以及尽快恢复正常业务的需要。

虽然 NCIRP 的主要内容是常规开展的各项行动，以及形成一个共同的运行图景，但该计划还侧重于对重大网络事件进行响应的机制。下表描述了 PPD-41 定义的网络事件和重大网络事件。联邦政府利用“网络事件严重度图示”（见附录 B）来认定事件级别及严重程度，并给出阈值，说明对什么样的重大网络事件可视为对美国或其海外利益造成影响。美国计算机应急准备小组（US-CERT）的网站还提供了一个列表，说明了网络事件一般而言如何发生及如何对信息和资产造成破坏<sup>①</sup>：

事 件	定 义
网络事件	是指在计算机网络中发生或通过其实施的，对计算机、信息或通信系统及网络控制的物理或虚拟基础设施，以及其上存储的信息的完整性、保密性或可用性已实际产生或即将产生危害的事件
重大网络事件	是指可能对美国的国家安全、外交关系或经济发展以及美国人民的公众信心、公民自由、公共健康与安全造成严重危害的网络事件或一组相关的网络事件

4. 与国家战备体系的关系

NCIRP 聚焦于网络事件响应，而国家战备体系则为更广泛的团体<sup>②</sup>如何预防、保护、减轻、响应、恢复网络事件建立了一个宽泛的框架。特别是“国家响应框架”（NRF），<sup>③</sup>为如何建立、维持和提供“按照国家战备目标”<sup>④</sup>中明确的响应核心职能提供了指南。为进一步将 NCIRP 与 NRF 联系起来，《国土安全法》<sup>⑤</sup>规定，DHS 部长要与其他相关联邦部、局负责人协调，按照 NCIRP 要求定期更新、维护及演练响应计划。NCIRP 采纳了 NRF 的理念、职能和组织结构等内容，因此 NRF 和 NCIRP 的结构都与国家事件管理体系（NIMS）保持一致。

NIMS 为包括联邦和 SLTT 政府在内的美国各级政府和私营部门提供了通用语言和事件管理结构，并定义了标准指挥和管理架构。成功的响应行动依赖于共同的、可互操作的方法来共享资源、实施协调以及交流信息。NIMS 为防止、保护、减轻、响应和恢复网络事件提出了举国<sup>⑥</sup>的综合方法，不论事件发生的原因、大小、位置或复杂性。

① <https://www.us-cert.gov/incident-notification-guidelines#attack-vectors-taxonomy>。

② 2016 年 8 月的“对联邦跨机构运行计划的响应”（第 2 版）对“整个团体”进行了描述，包括所有人以及家庭的各个成员，尤其是包含残障人士、儿童、老年人、英语熟练水平各不一致的人、社团、私营和非盈利行业、宗教信仰组织、地方政府、州政府、部落政府、领地政府、列岛区域以及联邦政府，也就是说，是整个国家。  
[https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response\\_FIOP\\_2nd.pdf](https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf)。

③ NRF 是国家战备体系的 5 个框架之一，描述了整个团体如何共同努力，以实现各个专门响应域的国家战备目标。<http://www.fema.gov/national-response-framework>。

④ <http://www.fema.gov/national-preparedness-goal>。

⑤ 《美国法典》第 6 编第 149 节。

⑥ 国家战备体系指的是整个团体，NCIRP 则描述了举国方法，这是由网络基础设施及其相关事件的特性决定的。国家战备体系中，支撑每个单元的指南、项目、流程以及体系都使得国家战备能够成为一种联合的、整个团体参与的方法，包括个人、家庭、社区、私营和非盈利行业、宗教信仰组织以及各级政府。  
[https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national\\_preparedness\\_system\\_final.pdf](https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf)。



所有的 NIMS 组成单元——资源管理、管理与协调、通信与信息管理等均提供了一个通用的框架。无论在何种司法管辖区及何种组织，无论其权限、管理结构、沟通能力、协议各不相同，但都可以彼此整合起来实现共同目标。这些概念也可用于网络事件响应，特别是在以下方面：

- 制定统一的事件目标集；
- 采用整合的战略方法来实施事件管理；
- 改进信息流，加强协调；
- 对优先级和局限性达成共识；
- 维护相关机构的法律授权；
- 使事件响应中所有参与者的联合努力得以优化。

国家响应框架包括 14 项“应急支持功能”（ESF）<sup>①</sup>，这些联邦协调架构可以将资源和能力集中到国家响应活动中最需要的领域。ESF 通过绑定和管理各项资源，提供了 NRF 所要求的核心功能。为了对事件响应提供支持，这 14 项 ESF 汇集了联邦各部、局以及其他国家层面资产的能力。ESF 不依靠单一政府部、局的能力，而是通过组织各方力量共同应对网络事件。

ESF 可由 DHS 的联邦应急管理局（FEMA）或应国土安全部长指示启动，并以各项事件响应活动为基础。具体而言，如果一个网络事件会产生对通信行业及其他的 ESF 领域的大规模物理破坏，则联邦政府可通过 ESF#2（通信）来协调对该事件的响应及恢复。在一个既有网络也有物理影响的事件中，本计划第 7 章“协调结构和整合”描述的重大网络事件响应机制应与已经建立的各项 ESF 相协调，以纳入 ESF#2。附录 C 对网络事件严重度图示与国家响应协调中心的激活等级进行了比较。国家响应协调中心是一个多部门组成的中心<sup>②</sup>，在发生重大事件和应急情况时，负责协调整个联邦的活动。

下章将介绍 PPD-41 提出的并行工作方案，并明确了联邦政府、SLTT 政府在网络事件响应中的角色和责任。不仅如此，还明确了私营部门的角色和责任，因为它们拥有、运行着国家的大多数关键基础设施。

## 5. 角色和责任

各类公共-私营部门组织每天都在通过各项并行工作来管理、响应和调查网络事件。在事件响应中，要行动统一，这就需要所有参与组织对其角色和责任理解一致，以保护国家免受恶意网络活动威胁，以及管理网络事件及其后果。

联邦政府拥有网络事件响应所需的各类能力和资源，这些能力和资源分布于各个网络安全中心，具体情况详见附录 E（联邦网络安全中心的角色）。为了明确应共同承担的网络安全责任，联邦政府根据威胁响应、资产响应、情报支持和受影响实体内部响应等 4 项并行工作来进行事件响应。

当网络事件影响到私营实体时，联邦政府通常不会在受影响实体的响应中发挥作用，但仍将关注受影响实体的响应行动，并与受影响实体进行适当的协调。在网络事件的严重程度可能升级时，联邦政府将按照本计划“范围”一节的内容，与受影响实体进行外部协调，并提供资

---

<sup>①</sup> <http://www.fema.gov/national-preparedness-resource-library>。

<sup>②</sup> 国家响应协调中心：[https://www.fema.gov/media-library-data/1440617086835-f6489d2de59dddeba8bebc9b4d419009/NRCC\\_July\\_2015.pdf](https://www.fema.gov/media-library-data/1440617086835-f6489d2de59dddeba8bebc9b4d419009/NRCC_July_2015.pdf)。

产响应、威胁响应和情报支持帮助。

网络事件可能由个人的网络活动或操作不当造成。如果受过教育，个人或家庭就可以显著降低网络事件产生的影响、破坏和损害。虽然大多数网络事件不需要普通公民进行协助，但很多事件处置可以降低网络事件对个人财产造成的风险和潜在影响。普通公民可在[www.ready.gov/cyber-attack](http://www.ready.gov/cyber-attack) 上查看在网络事件事前、事中和事后可利用的资源和指南。US-CERT 也向家庭用户提供了与家庭互联网连接相关的安全风险和对策信息<sup>①</sup>。

并行工作方向

NCIRP 提出的网络安全共同责任以及各项响应行动需要 3 个并行工作方向来实施：威胁响应、资产响应和情报支持。第 4 个工作方向是受影响实体的响应<sup>②</sup>。这些并行工作方向为促进各项响应活动能够协同一致提供了基础，使网络事件的事前、事中和事后响应工作得以协调一致。联邦和非联邦实体应对这些工作方向形成统一认识，以便在响应网络事件响应时更好地行动。下表列出了重大民用网络事件中的联邦领导机构<sup>③</sup>。

行动方向	联邦领导机构
威胁响应	司法部下属联邦调查局和国家网络调查联合特遣队
资产响应	国土安全部下属国家网络安全和通信整合中心
情报支持	国家情报总监办公室下属网络威胁情报整合中心
受影响实体响应	当某个联邦机构发生重大的网络事件时，该机构将对其响应负主要责任； 当私营实体发生重大的网络事件时，联邦政府通常不会在其响应中发挥直接作用，但与关键基础设施对口的相关政府部门（SSA）将协调政府的有关工作，以了解网络事件对私营部门关键基础设施业务和运行造成的潜在影响

威胁和资产响应者共同承担的责任和行动，包括但不限于：

- 与受影响实体沟通，了解网络事件的性质；
- 向受影响实体提供可用的联邦资源和能力指南；
- 及时将响应过程中的情报和信息通过适当渠道迅速传播；
- 促进与其他实体的信息共享和运行协调。

国际协调在各项工作中发挥着重要作用。鉴于互联网和通信基础设施的跨国性及美国私营部门的国际化和连通性，联邦政府在网络事件的威胁响应、资产响应和情报支持上，应与国际合作伙伴协调。

国务院（DOS）在包括网络问题在内的一切国际外交活动中代表美国。根据“网络空间国际战略”（2011），外交是应对国内外网络威胁和网络事件响应的重要和必要手段。国务院通过

① <https://www.us-cert.gov/Home-Network-Security>。

② PPD-41 “美国网络事件协调”。<https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>。

③ 根据 PDD-41 附录，对国防部、情报共同体遇到的重大网络事件，资产和威胁响应行动由这些机构自行领导，但必要时可得到其他联邦机构的支持。如果一个网络事件影响或可能影响某个关键基础设施部门，则领导机构还要协调与之相关的 SSA。

在全球大使馆的外交官和工作人员，为全天候网络事件响应提供国际外交支持。在国务院协调与网络事件相关外交事宜的同时，很多联邦部、局也在积极维护和利用多边和双边伙伴关系。此外，很多 ICT 行业的企业和提供商与重要的国际机构具有跨国业务和关系，包括与全世界政策部门和操作部门的互动。必要时，联邦部、局也可与私营部门实体开展国际合作，对网络事件响应中的国际事务予以支持。

### 威胁响应

威胁响应涉及执法机构和国防机构的很多资源及能力。威胁响应包括：调查、取证、分析、缓解等行动；遏制威胁者；溯源。这些都需要同资产响应行动进行信息共享，并做到操作同步。此外，威胁响应行动还包括在受影响实体现场开展某些执法和国家安全调查行动，以及关联相关事件，并识别还有哪些实体受到影响或可能受到影响。如前所述，威胁响应者和资产响应者应开展合作，在事件响应时保持行动统一。SLTT 和私营部门在与相关执法机构合作中扮演重要角色。DHS、DOJ、DoD、能源部（DOE）和情报共同体（IC）等在重大网络事件影响其职责或责任，或者外国势力、外国势力的代理有行动嫌疑时扮演重要的威胁响应角色。

#### （1）私营部门

私营部门实体可及时向执法机构或政府实体报告和分享网络事件及恶意网络活动信息，因此在威胁响应行动中扮演重要角色。同时，ICT 供应商和制造商，如互联网服务提供商、电信运营商、关键网络硬件制造商和主要软件公司，在威胁响应行动中也扮演着重要角色，因为威胁者可能利用这些系统实施破坏。向联邦政府报告网络事件的联络信息参见附录 D。在报告网络事件时，私营部门实体还应遵守监管要求及法律要求。私营部门网络安全从业者和供应商提供了很多关键服务（如安全托管服务、安全迹象发现和预警、网络安全评估、事件响应等），他们也可能拥有与恶意网络活动相关的信息，这对威胁响应行动至关重要。《网络安全信息共享法》（2015）为私营部门和某些 SLTT 政府组织提出了责任及其他法律保护条款，为联邦政府、SLTT 政府、私营部门之间的信息共享创造了重要条件<sup>①</sup>。

#### （2）州、地方、部落、领地政府

很多州和地方拥有关于未经授权访问或损坏计算机系统的刑事法规，这些法规适用于网络事件。国家的很多融合中心处于联邦和地方执法机构的交汇处，扮演着与联邦、SLTT 与私营部门合作伙伴之间进行威胁信息共享的角色。地方政府，特别是特大城市在地方响应行动中扮演着重要角色。通常情况下，普通公民和小企业不参与联邦执法或事件响应行动。地方政府有责任为联邦和州的执法部门及事件响应者提供沟通渠道。如（1）“私营部门”所述，《网络安全信息共享法》（2015）为私营部门和某些 SLTT 政府组织提出了责任和其他法律保护条款，为联邦政府、SLTT 政府、私营部门之间的信息共享创造了重要条件。

#### （3）联邦政府

为了应对网络事件，联邦执法机构在 SLTT 及联邦政府、国际合作场合以及私营部门实体之间跨部门工作，处理犯罪和国家安全网络威胁。联邦调查局、美国特勤局、美国移民和海关执法局（ICE）、国土安全调查局（HSI）等联邦执法机构，负责对涉及其调查管辖区的犯罪活动实施威胁响应行动并进行适当协调。要以非涉密形式在情报共同体同第一响应者之间共享行动信息，这对协调事件响应行动至关重要。

<sup>①</sup> 在《网络安全信息共享法》之下，协助非联邦实体同联邦实体共享网络威胁迹象信息和防御措施的进一步的信息和指南可见于 <https://www.us-cert.gov/ai>。

根据 PPD-41，当重大网络事件发生时，司法部将作为联邦领导机构，通过联邦调查局和国家网络调查联合特遣队开展响应工作。本计划第 7 章中“重大网络事件的运行协调”一节介绍了应对重大网络事件威胁时各响应方的具体责任及协调角色。

司法部的美国律师办公室及其刑事和国家安全处将与联邦执法机构合作，利用刑事和国家安全授权对网络威胁者进行调查、起诉、阻断和逮捕。依据法律程序获得的信息和证据将用于调查网络事件来源，以及收集相关网络威胁信息。如涉及刑事案件，司法部的“计算机黑客和知识产权项目”将对全国范围的网络起诉事项进行协调；如涉及国家安全威胁，则由司法部的“国家安全事务网络专业网”负责实施。此外，司法部通过联邦调查局和国家网络调查联合特遣队，可酌情与其他联邦机构共享调查信息和网络威胁情报，以协助其他联邦机构分析网络威胁和漏洞。联邦调查局下属 56 个地方办公室的网络工作部门可支撑 SLTT 执法机构与私营部门保持沟通并共享信息，包括提供培训和认证课程、协调国内网络威胁调查。

美国特勤处有一个“电子犯罪特别任务组”的全国范围网络，可将学术界、私营部门和 SLTT 执法机构的资源进行结合，以预防、侦测和调查电子犯罪，包括对关键基础设施和金融支付系统的潜在恐怖袭击。

国防部负责对影响其资产和信息网络（DoDIN）的网络事件进行威胁响应。国防部还可在联邦领导机构要求下，经由国防部官员批准或由总统指示，根据需求和现有能力向 DoDIN 以外的民事机构提供网络事件威胁响应服务。

### 资产响应

资产响应包括向受影响实体提供技术援助，降低脆弱性，确认其他受威胁实体并评估其存在的相同或类似脆弱性。该类行动还包括与受影响的实体沟通了解网络事件性质，向受影响的实体提供可用的联邦、SLTT 和私营部门资源和能力的指南，及时将新情报和信息通过适当渠道传播，促进与其他联邦政府、SLTT 和私营部门实体的信息共享和运行协调。关键资产响应行动还包括评估关键基础设施部门或区域的潜在风险，涉及潜在的事件级联影响、互依赖性影响等。要制定降低这些风险的行动方案，并及时提供可用的联邦、SLTT 和私营部门资源和能力的指南。

利益相关方在资产响应行动中的作用和责任各不相同，这充分体现了在保护国家免受网络事件影响上，齐心协力和共担责任的必要性。

#### （1）私营部门

私营部门，特别是关键基础设施的所有者和运营者，在应对网络事件中发挥着重要作用。小、中和大型私营部门实体通常是网络事件的首要 and 主要响应者。私营公司要对其系统的安全负责，它们通常在第一时间发现事件并处于最佳响应状态。在进行事件响应时，私营实体必须按照要求报告或披露网络事件相关信息。多数情况下，网络事件被视为常规事件，私营实体利用公司内部资源或在服务商协助下便可缓解影响。针对网络事件的常规信息共享即使不需要强制性报告，也可提醒其他受威胁实体，以减轻网络事件对其系统的潜在级联影响。

很多私营部门服务提供商和网络安全从业者都在提供关键的服务，如安全托管服务、提供迹象信息和预警、网络安全评估、事件响应等。这些私营部门的资源可增强其内部网络安全能力。

ICT 提供商和制造商，如互联网服务提供商、电信运营商、关键网络硬件制造商和主要软件公司等，在防御和应对恶意网络活动中发挥重要作用。这些私营部门实体与其他响应机构之间的有效协调往往是网络事件响应的关键。

关键基础设施的所有者和运营者可与 DHS 及各个 SSA 开展公共-私营合作，执行“国家

关键基础设施保护计划”(NIPP)<sup>①</sup>，以提升战备水平和做好风险管理。由于某些关键基础设施部门之间相互关联和互依赖，一些公司可向同行业或跨行业企业提供信息，以促进情报和信息共享，共同应对网络事件和威胁。各公司还要看一看，如何将国土安全部、SSA、联邦、SLTT 执法及反情报机构、信息共享和分析中心 (ISAC) 及其他信息共享和分析组织分享和接收信息。

多数私营部门通过 ISAC 进行信息共享。ISAC 是一种基于行业的信息共享和分析组织 (ISAO)，来自金融、服务、能源、航空行业等不同部门的实体在组织内进行信息共享。尽管很多组织已成为有效开展网络安全合作的驱动因素，但一些组织尚未符合特定行业的需求。来自不同地域、部门或组织的实体形成的 ISAO 都在收集、分析和传播网络威胁信息。不能加入 ISAC 但需要网络威胁信息的组织可加入成为 ISAO 会员。与 ISAC 不同，ISAO 不必与关键基础设施部门相关<sup>②</sup>。

在网络事件发生，特别是重大网络事件发生时，需要联邦政府、SLTT、行业监管机构以及多个关键基础设施部门间加强协调。除了响应受害者本身为私营企业的网络事件以外，私营实体也可参与私营部门服务商（特别是互联网服务提供商、安全托管服务商和其他技术供应商）提供支持的国家级事件响应。在这类事件中，私营部门经常向联邦和 SLTT 政策的战备和响应行动提供支持。联邦和 SLTT 监管机构也对某些关键基础设施部门的某些类型的网络事件提出了强制性报告要求。根据事件发生的关键基础设施部门和类型，某些响应行动需要监管机构的协调、批准或监管救济。

私营部门实体可酌情考虑通过内部、外包服务或聘请外部专家，为网络安全及事件处理提供安全保障。常备服务是一个实体的网络结构的一部分，鼓励私营部门实体与政府响应者共享网络事件的常备服务和信息。《网络安全信息共享法》(2015) 为私营部门和某些 SLTT 政府组织提出了责任和其他法律保护条款，为联邦政府、SLTT 政府、私营部门之间的信息共享创造了重要条件<sup>③</sup>。

## (2) 州、地方、部落、领地政府

保障公民的安全和福祉是美国各级政府的根本责任。为实现这个目标，每个 SLTT 政府的主要负责人、行政官员、民选官员和执行人员都有责任确保其管辖范围内的战备、响应和恢复行动有效开展。在网络事件发生时，标准的应急响应角色和责任可能不足以应对威胁。联邦各州都要制定一个计划，明确资产响应中州内各实体的角色。该计划应参照 NCIRP，并将其作为网络附件编入州应急管理计划。本计划的附录 G “制定内部网络事件响应计划” 为联邦各州制定网络事件响应计划提供了参考，包括针对网络事件的协调、识别、检测、减轻、响应和恢复等。

为了建立严格治理和报告机制，各个政府机关的负责人应指定本机构的响应联络人，并确保这些联络人的信息是最新的。在重大网络事件中，为了促进响应行动的协调，各负责人应预先指定一名政府响应高级官员。通常情况下，NCCIC 指定国土安全顾问作为其主要联络人。

治理是国家网络资产响应中的重要因素，包括编纂制定支持性的法律框架、政策、计划和程序，明确国家首席信息安全官的授权和责任。治理也包含了上述要素对行政下属部门、机构以及其州属实体（州和地方应急管理机构、执法、司法和立法分支机构、港口、机场等国家关

<sup>①</sup> 2013 版 NIPP 见于 <https://www.dhs.gov/national-infrastructure-protection-plan>。

<sup>②</sup> <https://www.dhs.gov/isao-faq>。

<sup>③</sup> 在《网络安全信息共享法》之下，协助非联邦实体同联邦实体共享网络威胁迹象信息和防御措施的进一步的信息和指南可见于 <https://www.us-cert.gov/ai>。

键基础设施)的管理。如(1)“私营部门”所述,《网络安全信息共享法》(2015)为私营部门和某些 SLTT 政府组织提出了责任和其他法律保护条款,为联邦政府、SLTT 政府、私营部门之间的信息共享创造了重要条件。

SLTT 可利用的资源包括但不限于以下方面:

- 地区级的国土安全办公室和融合中心。
- 国土安全部资助的州际 ISAC (MS-ISAC),它们可为 SLTT 政府网络安全提供支持<sup>①</sup>,并作为联邦节点交换重要信息,协调 SLTT 和联邦政府。各州均设有一名 MS-ISAC 主要成员,通常是州首席信息安全官员(CISO)。
- 地方政府有资格申请和领取城市安全行动补助,并鼓励将网络安全和培训计划纳入其支出。
- 国土安全部国家保护和计划署的外勤人员,包括:
  - 区域和地区级网络安全顾问。他们作为网络安全专家,与 SLTT 首席信息安全官、网络应急管理社区紧密合作。
  - 区域主管和保护安全顾问。他们作为关键基础设施保护专家,与州国土安全顾问紧密合作。
- 州长国土安全顾问委员会提供了一个平台,各州、领地和哥伦比亚特区的国土安全顾问通过该平台讨论国土安全问题,进行信息和专业知识共享,并向州长通报州内影响国土安全政策的问题。
- SLTT 政府协调委员会(SLTT GCC)通过将熟悉各个关键基础设施行业的专家在地理上聚在一起,强化了对各个关键基础设施部门的领导力架构,确保了 SLTT 官员在关键基础设施安全和韧性方面发挥着不可或缺的作用。

国民警卫队在国家层面和联邦层面扮演着双重角色。国民警卫队在关键响应行动上具有专长,也具有开展网络行动的专业知识和能力。在州长和副参谋长的指示下,国民警卫队可执行国家任务,包括支持民间机构的网络事件响应。特殊情况发生时,如法律许可,国民警卫队可按要求执行联邦服务或执行国防部交代的任务,包括支持联邦机构网络事件响应。

在网络事件发生时,可要求 SLTT 负责人及联络人向联邦各部、局提供与 SLTT 优先事项相关的战备和响应行动的建议以及有关支持和协助。网络事件可能导致级联或物理影响,导致 SLTT 采取非网络事件响应行动。即使网络事件不影响 SLTT 政府系统,主要负责人和联络人也应了解联邦政府的资产响应行动。一旦发生超出政府能力范围的网络事件,他们还应该准备好向联邦政府请求进一步的资源,如落实《Stafford 法》的要求。

### (3) 联邦政府

联邦对重大网络事件的资产响应行动涉及来自联邦各部、局以及私营部门的很多资源和能力。在网络事件响应中,联邦政府要与国内外合作伙伴(包括私营部门和政府机构)开展合作,开展对网络事件的评估、缓解、恢复等活动。根据 PPD-41,国土安全部作为资产响应行动的联邦领导机构,通过 NCCIC 开展工作。在重大网络事件发生时,资产响应中相关机构的具体责任和协调角色在第 7 章的“重大网络事件的运行协调”一节中进行了描述。

管理和预算办公室(OMB)及《联邦信息安全现代化法》(2014)要求联邦各部、局在严

---

<sup>①</sup> 如果一个 SLTT 政府欲对私营部门提供支持,这时并不需要 MS-ISAC 的帮助。当 SLTT 政府通过资产响应行动对私营企业的支持时,SLTT 应直接与 NCCIC 进行联络。

重网络事件发生 7 日内进行报告，并且每年向国会、国土安全部和 OMB 提交汇总报告<sup>①</sup>。一旦一个机构的最高级计算机安全事故响应小组（CSIRT）、安全运营中心或信息技术部门确认发生了网络事件，必须在 1 小时内通过 US-CERT 将涉及联邦政府信息系统的所有计算机安全事件（包括事件对保密性、完整性或可用性的影响）报告给国土安全部<sup>②</sup>。

国土安全部为国家网络安全响应工作提出了战略指导，推动开展全国性统一行动，并可协调所有联邦资源，以提升国家关键基础设施的安全性和韧性<sup>③</sup>。根据 2014 年《国家网络安全保护法》，通过 NCCIC，国土安全部成为了联邦和非联邦实体之间的一个接口，双方通过这个接口来共享网络安全风险、事件、分析和警告等相关信息<sup>④</sup>。NCCIC 积极促进信息共享，可帮助确认其他实体是否存在相同或类似脆弱性风险，并共享缓解风险的建议和最佳实践措施。NCCIC 将与 SSA 及来自多个机构的代表和私营部门紧密协调，共享联邦和非联邦实体的网络安全风险、事件、分析和预警等相关信息，促进联邦民事领域、SLTT 政府和私营部门之间的网络安全事件协调。联邦政府对私营部门的资产响应支持可以采取现场技术援助的形式，但这通常要取决于受影响实体的需求或得到其同意。

作为联邦的对外接口，SSA 要对其所对口行业的行动进行优先排序和协调，因此在部门协调中发挥着一定作用。SSA 在符合法定权限以及其他政策、指令或规定的前提下，履行事件管理职责，为对口的关键基础设施部门提供支持或技术协助，以确认脆弱性并在适宜时参与事件缓解行动。国土安全部要确保，各个关键基础设施部门应对网络事件的方法是一致、整合的，并且是一种举国方法，无论在工作层面还是消息传播层面。

经与相关的 SSA 合作，国土安全部还将协调政府资源，以了解网络事件对某个关键基础设施部门或跨关键基础设施部门造成的潜在业务和运行影响。相关 SSA 通常也要协调联邦政府内的有关工作，目的也是要了解网络事件对私营部门关键基础设施业务和运行的潜在影响。各 SSA 将得到国土安全部 NCCIC 和国家基础设施协调中心的支持，维护和提供影响关键基础设施的威胁、事件态势感知信息并促进信息共享，包括以准实时能力提供 SSA 报告，与国家响应协调中心向 FEMA ESF 提供的报告进行协调，要求提供和接收来自公共-私营部门关键基础设施合作伙伴提供的事件信息。由于 SSA 对私营行业通常拥有超越网络安全和韧性所需的权限、职责和伙伴关系，因此 SSA 在网络安全事件的技术响应以及减轻事件对关键基础设施部门的系统性影响方面发挥着主导作用。

在实施网络事件响应时，国土安全部还可与外国合作伙伴定期进行信息共享并协调事件响应行动，此类国际协调主要发生在 NCCIC 与其外国政府 CSIRT 相关方之间。商务部（DOC）将与联邦、国际和私营部门合作伙伴进行协调，研判网络事件对互联网生态系统的影响，包括域名系统以及主要的数字经济平台。通过国家电信和信息管理局及 NIST，DOC 可以作为国家

① 《联邦信息安全现代化法》，公法 113-282，2014 年 12 月 18 日，<https://www.congress.gov/bill/113th-congress/senate-bill/2521>。

② US-CERT 的联邦事件通告指南，<https://www.us-cert.gov/incident-notification-guidelines>。

③ PDD-21 “关键基础设施安全和韧性”，2013 年 2 月 12 日。PPD-12 也为其他联邦机构赋予了角色和职责。司法部、联邦调查局负责领导关键基础设施中的反恐、反情报调查以及其他有关执法事务。在关键基础设施中，国土安全部部长、司法部部长也联合实施其各自的职责。

④ 2014 年《国家网络安全保护法》，公法 113-282，2014 年 12 月 18 日，<http://www.gpo.gov/fdsys/pkg/PLAW-113publ282/pdf/PLAW-113publ282.pdf>。

网络安全风险管理措施中心，还可通过工业和安全局履行《国防生产法》<sup>①</sup>规定的职责，包括对关键基础设施提供支持。

在某些情况下，监管要求或合同要求可能对受影响实体的资产响应支持提出具体义务要求，如强制性报告或可能超出正常协商程序的国家安全决定。此外，联邦监管机构如果具有相关权限，也应尽早参与事件响应，以快速执行豁免、审批、通知等事项。在重大网络事件中，必要时监管机构也可推动其所监管行业内的一致行动。

国防部（DoD）负责对受影响的军事资产和 DoDIN 进行资产响应。应其他联邦领导机构请求，并经由国防部官员批准或由总统指示，国防部还可根据需求和现有能力向民事领域提供网络事件响应支持。

情报共同体安全协调中心（IC SCC）负责对受影响的情报共同体资产进行资产响应。通过情报共同体安全协调中心，国家情报总监办公室（ODNI）可与情报共同体的任务合作伙伴进行合作，并得到其他联邦机构的支持，以管理情报共同体信息环境综合防御所面临的威胁并实施资产响应。

### 情报支持

情报及相关行动为更好地了解和利用现有的外交、经济或军事能力来响应网络事件，并与其他潜在受影响实体或响应者共享威胁和缓解信息等发挥了重要作用。特别是在重大网络事件中，资产和威胁响应者应利用情报支持行动建立威胁态势感知，共享相关威胁迹象和分析信息，识别和确认差距，并最终勾勒一张网络事件全貌图。

#### （1）州、地方、部落、领地政府

国家融合中心涉及州各级政府、私营部门实体和公众，各方的参与程度根据具体情况而有所不同。至少应在州级范围内组织和协调有关的融合程序，各州应为此建立和维护一个融合中心。尽管执法情报部门是融合中心的基础，但中心领导可根据对其各自辖区的评估，确定应参与融合中心工作的公共安全和私营部门实体。

#### （2）联邦政府

国家情报总监办公室通过网络威胁情报整合中心（CTIIC）向联邦机构提供网络事件情报支持。根据 PPD-41，一旦发生重大网络事件，国家情报总监办公室将作为联邦领导机构，通过网络威胁情报整合中心开展情报支持及相关行动。国家情报总监办公室的具体责任和角色在本计划第 7 章的“重大网络事件中的业务协调”一节中进行描述。

在情报支持行动中，CTIIC 将协调其他联邦网络安全中心和联邦利益相关方来获取联邦情报信息。CTIIC 也将通过国家网络情报管理员协调事件响应中的情报收集活动。

各情报业务中心都有为其提供情报支持的机构。根据《美国法典》第 6 编<sup>②</sup>，国土安全部情报和分析办公室负责向 SLTT 和私营部门合作伙伴提供情报，并从这些合作伙伴处收集情报，以支持国土安全部和情报共同体的工作。此外，国土安全部情报和分析办公室可向 NCCIC 的私营部门信息共享任务提供情报支持，如收集关键私营部门企业的情报需求，但该支持需要得到国土安全部国家保护和计划署的批准。

FBI 与其国内人员和分配到世界各地执法联络办公室的 FBI 工作人员之间收集和协调相关

---

① 1950 年《国防生产法》，2009 年 10 月修订（《美国法典》第 50 编 2061 附录及后款）。

② 《美国法典》第 6 编第 124a 节。



情报及其他共享信息，协调联邦机构与国际情报和执法部门之间的情报信息共享，生产和共享情报分析产品，包括对美国国土产生威胁的信息，此外还对相关的规划、能力建设和业务行动提供情报支持。FBI 还与 ODNI 任务和支持中心进行协调，为国土安全合作伙伴提供专项能力支持<sup>①</sup>。

NSA 所属的网络安全威胁运行中心（NCTOC）是 NSA 全天候（7×24 小时×365 天）跟踪和评估外国网络安全威胁的机构。NCTOC 通过对外国情报的分析，向合作伙伴通报当前和潜在的恶意网络活动，重点包括敌对计算机网络攻击、攻击者能力和实施破坏途径等。NCTOC 也会根据要求向美国政府各部、局提供技术援助。

DoD 负责积极跟踪和评估外国网络安全威胁，并向相关的跨机构伙伴通报当前和潜在的恶意网络活动。国防部情报部门可按要求向美国政府各部、局提供技术援助，其他国防部机构可根据法律和政策向民事机构提供支持。如果某信息显示，SLTT、关键基础设施所有者或运营者、其他私营部门实体可能会遭到确凿无疑的网络威胁，情报共同体可对此信息进行标密。根据第 13636 号行政命令第 4 节，国土安全部和 FBI 可向目标实体通报网络威胁<sup>②</sup>。必要时，也可提供脱密的威胁检测和威胁缓解相关信息。涉及国家安全威胁的来源认定、对手性质等的事件响应程序和规程应遵循国家安全处理事项的指南及规定。

### 受影响实体的响应

受重大网络事件影响的实体通常要根据相关法律、法规或合同义务，采取行动来管理网络事件对其运营、客户和员工的影响。当受影响实体是联邦机构时，该机构有责任尽一切努力来管理网络事件的影响，这些努力可能包括但不限于：

- 维持业务或运行的连续性；
- 降低潜在的健康和安全影响；
- 处理不利的财务影响；
- 保护隐私；
- 管理责任风险；
- 遵守法律和法规要求（包括披露和通知）；
- 与员工或其他受影响人员沟通；
- 处理外部事务（如媒体和国会调查）。

当受影响实体是私营实体时，联邦政府通常不会在受影响实体的响应中发挥作用，但仍将关注受影响实体的响应行动，遵循上述原则与受影响实体协调。与关键基础设施对口的政府部门将协调联邦政府的工作，以便了解网络事件对私营部门关键基础设施在业务或运行方面的潜在影响。

### 涉及个人身份信息的网络事件

按照管理和预算办公室 M-07-1612 号备忘录“保护个人信息并对信息泄露进行响应”（及其后续修订版本），以及管理和预算办公室制定的“信息泄露响应计划”，一旦发生影响民事联邦政府机构的网络事件，且有事实或证据显示该网络事件涉及个人信息，应通知负责

① 2004 年的《情报改革和预防恐怖主义法》（公法 108-458）第二章第 118 节第 3638 行，列出了 FBI 的情报授权，12333 号行政令与此一致。《美国法典》第 50 编第 401 节后续条款以及《美国法典》第 50 编第 1801 节后续条款对此均有描述。

② NCJITF 已经实施了第 13636 号行政令的 4（b）款，以记录这些通知的产生、传播和处置过程。

隐私的高级机构官员，并对个人身份信息泄露事件采取一切必要的响应行动<sup>①</sup>。

## 6. 核心功能

核心功能是针对网络事件实施威胁响应、资产响应和情报支持的关键要素，是各级政府在网络事件响应中必须具备的功能，它采用通用语言描述了必须在全国范围执行的重要能力。

核心功能可通过适当地规划、组织和培训人员，或通过部署 NIST 网络安全框架或私营部门开发的网络安全行动来实现。国家战备目标将核心功能添加到了行动任务中，具体内容详见附录 H（核心功能、NIST 网络安全框架、PPD-41）。

本节将简要描述这些功能，具体内容详见附录 F（核心功能以及符合国家战备目标的核心功能）<sup>②</sup>。附录 F 并非详尽的能力清单，它描述了针对特定需求应该开发和加以利用的能力以及应对网络事件的角色、责任和权限。各级政府、私营和非营利部门组织、关键基础设施所有者和运营者，都要评估其自己面临的风险，确认其所需具备的核心功能。附录 I 描述了私营—公共部门可以利用的其他资源，这些资源也可用于了解网络事件响应、漏洞更新、数据泄露信息、风险管理、有关机构等。

与应对其他威胁和危害的事件响应一样，网络事件响应是相关各方共同的责任。举国必须共同努力，确保美国为应对网络事件做好了准备。同时，我们应意识到，不是每个网络或系统都面临相同的风险。通过举国共同努力，建立和提供网络响应核心功能，美国可以更好地应对威胁，协助恢复基础服务和公共功能，以及促进各类恢复行动的整合。

### （1）访问控制和身份验证

这是指，采用并支持必要的物理、技术和网络措施来控制对关键位置和系统的准入，这也被称为鉴别和授权。该功能通过实现和维护相关协议来验证身份，授权、给予或拒绝对特定 IT 系统和网络的访问。

### （2）网络安全

这是指保护（或必要时恢复）计算机网络、电子通信系统、信息和服务免受损坏、非授权使用和恶意利用。更多的时候，网络安全也被称为信息安全，它通过多项活动和工作来确保关键信息、记录、通信系统和服务的安全性、可靠性、保密性、完整性和可用性。

### （3）取证和溯源

针对事件的取证调查和溯源是重大网络事件中并行开展的互补功能。

- 取证：即通过科学的、基于情报的敏锐度来发现和识别与被调查事项相关的信息。针对网络事件，取证涉及数据复制、提取和分析等一系列学科，以发现和识别恶意网络活动的相关线索。取证也包括一些子学科，如基于主机的取证、网络和数据包数据取证、内存分析、数据关联和恶意软件分析。

在重大网络事件响应中，政府机构和私营部门合作伙伴经常同时进行分析并将分析结果共享，以便就恶意网络活动和如何防范类似活动达成共识。在事件发生以后，不同的威胁、资产和业务响应组织也可以开展取证分析。尽管这些行动看似重复，但其结果会因实体的职能和资源各异而各具特点。

---

① OMB 第 M-07-16 号备忘录“保护个人身份信息并对信息泄露进行响应”，2007 年 5 月 22 日。

② <https://www.fema.gov/core-capabilities>。

- 溯源：即识别与特定事件相关联的对手，它是对收集的证据和情报进行分析后得出的结果，以识别造成网络事件的个人或组织。溯源发生在调查的生命周期的后期，有时在网络事件响应开始时可能无法溯源。虽然针对重大网络事件开展溯源行动是联邦响应机构的主要职能之一，但其他政府和私营部门实体在事件溯源中也扮演着重要角色。

对事件源头的评估不仅对执行刑事或国家安全调查的政府机构很重要，对受影响实体也很重要。受影响实体可根据证据考虑是否对威胁者发起其他的法律或民事诉讼。

该核心功能还包括在事件期间支持计算机网络和资产分析的独特且技术性的行动。这些支持行动有助于了解当前威胁的各方面情况，便于减少当前事件的影响以及防止网络事件在网络空间进一步传播。

#### （4）基础设施系统

恶意网络活动发生后，要将关键基础设施功能稳定下来，减少对健康和安全的威胁，有效地响应和恢复系统和服务，以支持可靠、富有韧性的系统。关键的基础设施和网络相互依存。在网络事件的响应中，该功能聚焦于保护设施资产和实体、修复损坏的资产、重新获得对远程资产的控制，以及评估整个关键基础设施部门的潜在风险。

#### （5）情报与信息共享

这是指基于规划、指导、收集、开发、处理、分析、生产、传播、评估以及对针对美国及其人民、财产利益的恶意网络活动的反馈，提供及时、准确和可操作的信息。情报和信息共享是必要时在政府或私营部门实体之间交换情报、信息、数据或知识的功能。

针对网络事件，该功能涉及联邦要与 SLTT 实体、私营部门和国际合作伙伴有效进行情报交流和其他信息的收集与共享，以便形成对美国潜在网络威胁的态势感知。

#### （6）拦截和阻断

这是指延迟、转移、拦截、阻断、逮捕与恶意网络活动相关的威胁。由人、软件、硬件或行动产生的网络事件可对国家网络和基础设施造成威胁。同时，某些威胁可能源于应对网络威胁采取的拦截和阻断行动。拦截和阻断包括对人员、项目或设备采取制止或阻止行动，并利用技术手段或其他手段来防止恶意网络活动。该功能有助于阻止和消除即将形成的网络威胁，并可用于保存证据和为政府检控违法者提供支持。

#### （7）物流与供应链管理

这是指促进和协助基本商品、设备和服务的交付，以支持受影响的系统和网络的响应。

针对网络事件，该功能聚焦于提供物流或业务支持，实现由领导层确定的网络事件响应优先事项，包括对实时响应资源需求的识别、优先排序和协调。

#### （8）通信

这是指采取一切可行手段，确保受影响实体和所有响应者之间进行及时通信，以支持安全、态势感知和运营。

针对网络事件，该功能包括利用内部互操作语音、视频和数据系统及网络，识别对有效响应网络事件至关重要的联邦支撑性组织、功能和团队。在网络事件中，该功能聚焦于及时、动态、可靠地运行和处理事件信息，以满足各级政府及授权参与的私营部门合作伙伴组织决策者的需求。

#### （9）运行协调

这是指建立和维护统一的、一致的运行结构和流程，整合所有关键利益相关方，并支持核心功能的实施。该功能可支持全国范围各类决策者采取适当的行动并监督其复杂的业务操

作，以实现工作的一致性，产生良好效果。运行协调将遵循 NIMS 和事件指挥系统的原则，在网络事件或针对美国境内的恐怖主义行为中，协调威胁响应、资产响应和情报支持活动。“消息的统一性”在指导原则中已介绍，相关信息详见附录 D（向联邦政府报告网络事件）。针对网络事件，该核心功能将涉及协调各级政府和私营部门合作伙伴之间的行动。

#### （10）规划

这是指执行系统性的流程，使举国参与到制定可执行战略、操作或战术层面的方法上来，以实现既定目标。

针对网络事件，规划包括全面规划和事件行动规划。全面规划涉及发展战略、运营和战术的规划，旨在防止、保护、减轻、响应和恢复网络事件。事件行动规划即在有时间限制的环境下，制定或迅速调整操作和战术计划，对即将发生或正在发生的网络事件做出响应。

#### （11）公共信息和预警

这是指采取清晰、一致、可访问的、符合文化和语言习惯的方法，适时向全国和公众发布统一、及时、可靠并可操作的信息，旨在有效传播关于重大威胁或恶意网络活动的信息，或是正在采取行动和提供援助的相关信息<sup>①</sup>。

针对重大网络事件，该功能将采用有效的和可访问的迹象指示和预警系统，向受到或潜在受到重大网络事件影响的运行者、安全官员和公众通报重要网络威胁信息。

#### （12）筛选、搜索和检测

这是指通过主动和被动的监视及搜索程序来识别、发现或定位恶意网络活动的威胁，包括采取系统性检查和评估、传感器技术或物理调查和情报等方法。

针对网络事件，该功能包括当有可靠情报显示出可能的攻击目标、恶意网络行动类型或威胁行为体时，要采取针对性的行动，核实或描述已经发现的网络威胁。对网络事件的筛选可采用网络状态、资产、传感器监控和其他可提供安全状态信息的技术。

#### （13）态势评估

这是指向所有决策者及时提供恶意网络活动的性质和范围、级联效应以及响应状态的决策信息。

针对网络事件，该功能聚焦于快速处理和传达从国家层面到现场层面收到的大量信息，为所有决策者提供最新和最准确的信息。

#### （14）威胁和危害识别

这是指识别影响网络和系统的恶意网络活动威胁，确定这些威胁的频率和量级，并将其纳入分析和规划流程，以便清楚地了解各实体的需求。

针对网络事件，该功能涉及持续、及时准确地收集网络威胁信息，包括评估技术进步带来的影响，以满足分析师和决策者的需求。标准化的数据集、平台、方法、术语、指标和报告可以使这项工作更有效，以统一各级政府和私营部门的工作，减少冗余。

## 7. 协调结构和整合

本文第 2 章“简介”中已经提到，成功管理网络事件需要采用一种举国的方法，促进私营

---

① 美国总统已指示国土安全部部长和司法部部长进行彼此协调，承担起向国家提供关于威胁和事件的公共信息和预警的职能。

部门、SLTT 政府、联邦机构和国际合作伙伴等所有利益相关方之间的协调。通过已建立的协调结构来管理、协调各实体，从而形成合力响应网络事件。

协调结构为受网络事件影响或负责网络事件响应的实体代表提供了一种机制，以助其开展协调和响应行动，包括战备活动、职能交付、制定运行计划、协调响应人员和响应行动、编制统一的公共消息和警报规范以及权衡不同行动可能带来的技术、运行、政治和政策影响。

现有的政策和协调结构已可以处理绝大多数网络事件，但重大网络事件可能需要采用特定的方法来协调举国的响应。根据 PPD-41，美国政府将建立一个网络统一协调小组（UCG），负责在重大网络事件响应过程中协调各联邦机构，并将 SLTT 政府和私营部门合作伙伴纳入事件响应工作中。其他协调结构应做好与网络 UCG 进行整合和互操作的准备。

本节介绍了为响应网络事件，各利益相关方在需要外部配合时可参考的主要协调结构，具体描述了如何利用这些结构并结合其他结构，做好重大网络事件响应的运行协调。

### 协调结构

为有效响应网络事件，各利益相关方可利用现有的各种协调结构，来促进信息共享、协调响应行动、获取技术援助和其他资源、提供政策协调和指导。平日发生的大多数网络事件都可被视为常规事件，可由受影响实体内部处理。受影响实体可根据事件的性质、具体组织或部门的需求，在以下协调结构中选择所需的一种或多种结构。对于涉及国家安全或公众卫生 and 安全的网络事件或重大网络事件，PPD-41 明确了联邦领导机构，并给出了一个协调结构框架，该框架是通过网络 UCG 制定运行响应计划并协调响应行动。

#### （1）私营部门

多年来，私营部门成功参与了产业和政府之间的协调工作，通过信息共享、分析和协作，发现、预防、减轻和响应网络事件。PPD-21 “关键基础设施安全和韧性”<sup>①</sup>指定的 16 个关键基础设施部门和子行业均设有独立的部门协调理事会（SCC），会员包括关键基础设施所有者和运营者、产业贸易协会和私营部门实体。各个 SCC 实际上是为其成员提供了一个论坛，推动其成员之间、与政府协调委员会之间和与 SSA 之间进行合作，解决本关键基础设施部门所特有的以及跨基础设施部门的安全及韧性相关政策与战略问题。

此外，通过已建立各信息共享与分析中心（ISAC），私营部门关键基础设施社区也已开展了协调工作。ISAC（不包括州际 ISAC）由私营部门组织和管理，支持与关键基础设施保护和网络安全有关的公共-私营合作关系。“ISAC 国家理事会”将继续促进跨基础设施部门协调，推动私营部门与联邦、州和地方政府之间开展富有成效的合作。

如前所述，根据第 13691 号行政令，国土安全部正积极制定标识程序，以创建信息共享和分析组织（ISAO）<sup>②</sup>，并对各 ISAO 进行认可，使各利益相关方可以基于彼此之间的某种密切关系（如地理上相近，处于同一行业或社区，或面临共同的威胁）建立若干信息共享小组，以提供更为正式的信息共享结构和技术援助条款。已建立信息共享机制并每天进行信息共享的组织，可被视为 ISAO 或 ISAC，或其中的成员。虽早于 ISAO 出现，但 ISAC 也是一种 ISAO。

① <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>。

② [www.isao.org](http://www.isao.org)。

## （2）州、地方、部落、领地（SLTT）政府

州、地方、部落、领地（SLTT）政府也拥有各类可用于网络事件响应的协调结构，以支持参与者之间协作开展信息共享、事件响应、运行协调和政策活动。与私营部门组织一样，SLTT 政府可以成为 ISAC、ISAO 或其他信息共享组织的成员，也可以在国家政策协调层面成为 SLTT 政府协调委员会的成员。针对 SLTT 政府网络中发生的事件，州际 ISAC 已与联邦政府建立了联系，并将向其会员提供信息共享和技术援助。作为关键基础设施和重要资源的所有者和运营者，相关 SLTT 政府机构也可成为其对口的 ISAC 的会员，并可设立与其行政管辖权一致的协调结构，以便针对网络事件向响应官员提供协调和指导。很多 SLTT 政府还通过选定的网络信息共享小组开展合作，如“州首席信息官员全国协会”或“全国州长协会”。

虽然很多 SLTT 政府正在建立和应用网络事件响应的业务协调结构，但并未采用标准方法。一些 SLTT 政府将州或主要城市的融合中心作为主要联络和信息共享枢纽，另一些则选择各自的应急或安全运营中心。对于造成物理影响的网络事件或必须与其他应急管理机构（如消防部门、公共卫生机构及人力服务机构）合作响应的网络事件，应急运营中心应提供重要信息共享和事件管理功能。

在州/领地级政府层面，应急行动中心经常同联邦机构（包括 FEMA 和国防部）协调所需的资源，并与国民警卫队进行业务协调。鼓励 SLTT 为其应急行动中心的员工提供相关网络安全培训，网络事件响应者也应根据需要接受应急响应和应急运营中心的培训。

## （3）联邦政府

联邦政府将网络事件响应的协调结构分为以下 3 类：

- 通过网络响应小组（CRG）<sup>①</sup>开展的国家政策层面的协调；
- 通过联邦网络安全中心和各联邦机构开展的业务协调；
- 通过与关键基础设施对口的政府部门（SSA）和政府协调委员会（GCC）开展的部门协调。

为开展国家层面的政策协调，PPD-41 指派总统国土安全和反恐助理负责召集和领导网络响应小组（CRG），针对影响美国国家利益或海外利益的重大网络事件，协调制定和实施联邦政府政策和战略。CRG 将负责协调制定和实施美国政府应对重大网络事件的政策和战略。可邀请联邦各部、局（包括相关网络安全中心），根据其在各类网络事件响应中扮演的角色、承担的责任和专长，参与 CRG。定期参与 CRG 的联邦机构（包括 SSA），必须建立和实施增强性协调程序，以管理超过其常规响应能力的重大网络事件。

目前，联邦政府已建立了 7 个网络安全中心，其职责包括实施网络行动、加强信息共享、维持态势感知，并已成为公共-私营部门实体之间的联络渠道。所有安全中心应与联邦实体协作，并在经过允许和授权情况下，为网络事件响应提供支持。根据 PPD-41，上述中心中的 3 家，包括国家网络安全和通信整合中心（NCCIC）、国家网络调查联合特遣队（NCIJTF）和网

---

① 网络响应小组（CRG）的更多信息参见 PPD-41 “美国网络事件协调”，<https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination, <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>。

络威胁情报整合中心（CTIIC），负责协调网络 UCG 内部对重大网络事件的响应行动。

此外，联邦政府还指派了一些对口的政府部门（SSA）来领导其对口的关键基础设施部门的政府协调委员会（GCC）。根据 PPD-21，16 个关键基础设施部门均设有 SSA。各 SSA 利用其专业知识和技能，负责向其关键基础设施部门提供信息共享、协调、事件响应和技术援助，具体参见 PPD-21 和 NIPP。GCC 则包括其他具有权限和技能的政府机构，通过广泛吸纳适宜的机构（包括联邦和 SLTT 政府），GCC 成员的积极参与将实现机构间和行政区间的协调。

#### （4）国际

国际信息共享可通过公共和私营部门的大量机制开展。很多组织拥有涉及国际合作企业和政府的信息共享关系。国际业务协调可借助联邦各部、局与外国同类机构或国际组织的关系，通过由国务院管理的正式外交渠道开展，也可通过私营企业与其他私营部门实体、国家政府和国际组织之间的国际关系开展。

很多联邦机构和网络安全中心都与外国同类机构保持联系，在稳定状态或网络事件发生时均进行信息共享及合作。为促进国际调查，联邦执法机构也与外国同类机构、国际刑警组织保持信息共享渠道。联邦调查局依据其“法律专员计划”，在驻外美国使馆设立了网络联络处。国土安全部或 ICE HSI 拥有广泛的法律权限来执行联邦法规，并利用这些权限调查各类的跨国犯罪活动。美国特勤局通过海外办事处，或通过协同国际工作组部署电子犯罪特工计划，最大程度地与国际执法机构建立伙伴关系。NCCIC 与国际计算机安全事故响应小组（CSIRT）伙伴合作，获取态势感知信息并确定保护和响应的优先事项。国务院海外安全咨询委员会等组织，通过产业代表委员会或由美国大使馆及其他外交途径建立的渠道，协调信息共享、安全行动合作和美国私营部门海外利益分析。此外，一些 ISAC 在保护美国参与者信息的基础上已经向友国的公司和组织开放会员资格。

鉴于现有关系已有多种，并考虑到重大事件的响应中会出现很多政策或操作方面的重叠问题，为此必须强调国际合作很有可能会通过多条渠道并行开展。

### 重大网络事件的运行协调

网络事件会持续影响国内利益相关者。绝大多数网络事件对美国国家安全利益、对外关系、经济发展、公众信心、公民自由或公众健康和安全没有明显威胁，不属于 PPD-41 和“网络事件严重度图示”（附录 B）定义的重大网络事件。该类网络事件可由受影响单位独立解决，也可通过其他私营部门利益相关者、联邦或国际政府机构提供常规支援解决。当重大网络事件发生时，联邦政府可组建一个网络 UCG，作为协调联邦机构内部和联邦机构间响应活动的主要方式，并酌情将相关私营部门合作伙伴纳入工作组。

#### （1）确定事件严重程度

联邦政府采用“网络事件严重度图示”（附录 B）作为通用框架来确定网络事件的严重程度，并在联邦部、局层面共享对网络事件的评估与评价。评级在 3 级及以上的网络事件视为重大网络事件。为有效解决事件，联邦政府各部、局在评估网络事件的严重程度和潜在影响时，均应采用“网络事件严重度图示”，确保术语统一，信息共享适当，管理适宜。如前所述，附录 C 对网络事件严重度图示与国家响应协调中心的激活等级进行了比较，以便结合网络事件和

物理事件响应。联邦网络安全中心（NCCIC、NCIJTF 和 CTIIC）作为 PPD-41 指定的联邦领导机构，通过协商评估潜在重大事件的严重程度。

美国的关键基础设施部门由公共的和私营的所有者或运营者组成，双方均提供着重要服务，并拥有联邦政府和国家十分依赖的独特专长和经验。如果事件已经影响或可能影响属于一个或多个关键基础设施部门的非联邦实体，国土安全部（DHS）将通过其下属 NCCIC 和受影响或潜在受影响关键基础设施对口的 SSA 来确定事件的严重程度，必要时可通过关键基础设施部门 ISAC、SCC、GCC、ISAC 全国委员会、州际 ISAC 或关键基础设施安全合作伙伴等组织，向关键基础设施部门的权威组织、关键基础设施所有者和运营者咨询。私营部门评估有助于使 NCCIC 了解网络事件的严重等级。

由于私营部门拥有和运营着绝大多数关键基础设施，多数情况下，联邦政府了解潜在的重大网络事件的途径是受影响实体或部门的自愿报告和通过协调机制进行的信息共享。联邦政府也鼓励非联邦实体采用网络事件严重度图示或 NCCIC 网络事件评分系统<sup>①</sup>进行评估，以提供一个可重复的且一致的评估事件风险的机制。

此外，当重大网络事件影响私营部门利益相关方、SLTT 政府或国际同类机构时，它们可通过以下几种途径与联邦政府自愿共享信息：

- NCCIC、FBI 或 NCIJTF；
- 相关 SSA 或监管机构；
- 联邦执法机构驻当地办事处，包括 FBI、美国特勤局、美国 ICE/HSI 或相关军事刑事调查组织。

有关联络人员向联邦政府实体报告事件的内容参见附录 D “向联邦政府报告网络事件”。除自愿报告外，根据法律、法规或者合同，具有强制性报告要求的受影响实体必须履行其义务。

接到报告的联邦机构应与其他联邦机构协调响应网络事件，包括确定是否建立网络 UCG 来协调重大网络事件响应。作为决策过程的一环，利益相关方可向联邦机构提供信息和评估意见，说明其对其实体及其部门的事件严重程度的看法。在此过程中，联邦机构也会参考受影响实体的意见。同时，联邦政府还将向相关的私营部门组织、ISAC、ISAO、SCC、SLTT 政府和（或）国际利益相关方进行咨询，以了解事件的严重程度和影响范围。

## （2）增强性协调程序

根据 PPD-41，经常参与网络响应小组（CRG）（包括相关 SSA）事务的联邦机构应确保其具有在网络事件响应中发挥作用的常备能力。各机构应制定增强性协调程序，为超过其常备能力的重大网络事件响应行动做好准备。这些程序需要专门的领导、支持人员、可用设施（包括物理和通信设施）以及内部流程，使其能够管理超出其正常运行条件，并对协调能力有较大需求的重大网络事件。

增强性协调程序有助于：

- 在重大网络事件期间，确立与其他联邦机构（包括相关机构联络人）进行通信，并通知 CRG 增强性程序已激活或启动的适当途径。

---

① 国家网络事件评分系统，<https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>。



- 对有效的事件协调所需的内部沟通和决策流程予以强化。
- 制定维护这些流程的程序。

此外，为根据 PPD-41 协调网络事件响应行动，各联邦机构的增强性协调程序都明确了该机构的流程和现有职能。政府和私营部门员工应获得必要的许可和访问授权，以便及时共享信息。PPD-41 还要求各 SSA 制定或更新能反映其对口关键基础设施的特点的流程，必要时可与对口的关键基础设施部门协商，以增强对重大网络事件响应行动的协调。这些聚焦关键基础设施的流程是将政府和私营部门响应流程（包括确定重大网络事件业务影响并对其响应的流程）相结合的关键机制。

### （3）网络统一协调小组（UCG）

根据 PPD-41 要求，网络 UCG 将作为联邦机构内部和机构间主要的国家运行协调机制，负责在重大网络事件期间标识和制定运行级的响应规划及行动，以及在必要时将私营部门合作伙伴与 SLTT 整合到网络响应工作之中。

#### ①权限

网络 UCG 是为威胁响应、资产响应和情报支持建立共同目标，以指导中短期的网络事件响应和恢复工作。PPD-41 要求组建网络 UCG 并设计了其运行概念。PPD-41 不会改变、取代或限制联邦机构参照法律、其他总统指南和指令履行其职能和职责的权限。相反，PPD-41 建立在 PPD-8 “国家战备”的基础之上，通过整合网络 and 传统战备工作来管理网络事件和物理事件，它还参考了 SSA 结构和 PPD-21 “关键基础设施安全和韧性”中的任务分配。网络 UCG 旨在形成合力，一般不改变机构的权限或其领导、监督、指挥的责任，除非相关机构负责人共同同意并符合适用的法律（包括《1932 年经济法案》）要求。

#### ②网络 UCG 的成立

只有在发生重大网络事件时，网络 UCG 才会成立和激活，成立后也只负责特定事件的响应。网络 UCG 可通过以下流程成立：

- 由国家安全会议的主管委员会（部长级）、代表委员会（安全代表级）或网络响应小组（CRG）指导成立。
- 两个或多个经常参与 CRG 事务的联邦机构（包括相关 SSA）使用网络事件严重度图示评估后认为必要，应成立网络 UCG。
- 或当重大网络事件影响关键基础设施所有者和运营者时，如果国土安全部部长确定该重大网络事件可能对公众健康或安全、经济安全或国家安全造成区域级或国家级的灾难性影响，也应成立网络 UCG。

当不再需要威胁响应和资产响应的增强性协调程序，或单一联邦机构的权限、职能或资源就足以管理联邦针对事件的响应行动时，网络 UCG 将解散。

#### ③网络 UCG 的责任

根据 PPD-41，网络 UCG 应采取以下行动，促进重大网络事件响应行动的协调一致：

- 遵循 PPD-41 附录第 3 节所述原则协调网络事件响应。
- 确保将所有相关的联邦机构，包括 SSA 纳入事件响应。
- 协调制定和执行响应和恢复任务、确定优先事项和制定行动计划，包括国际和跨部门

的外联行动，以促进对事件的恰当响应和快速恢复。

- 促进在网络 UCG 内部迅速、恰当地分享关于事件响应和恢复行动的信息和情报。
- 针对某事件，协调与受影响或可能受影响的部门、利益相关方（必要时也包括公众），进行一致、准确和适宜的沟通。
- 发生既有网络影响也有物理影响的事件时，成立联合 UCG，可联合联邦领导机构，也可联合 PPD-8 “国家战备”<sup>①</sup>中网络应急框架（或其他可能适用的行政令）给出的对管理该事件物理影响的 UCG。

针对已确认的潜在法律问题，网络 UCG 将根据情况及时协调司法部、国土安全部总法律顾问、监管机构以及其他相关联邦机构的律师，以便必要时协同相关的非政府实体，快速考虑并协调解决上述问题。

#### ④网络 UCG 的参与

根据 PPD-41，当网络 UCG 成立时，联邦政府设立 3 个领导机构，以有效应对重大网络事件：

- 国土安全部（DHS）：是重大网络事件资产响应行动的领导机构，通过国家网络安全和通信整合中心（NCCIC）开展工作。NCCIC 包括私营部门、SLTT 和众多联邦机构的代表，它是联邦实体与非联邦实体间共享网络安全风险、事件、分析和警告等信息的关键节点。
- 司法部（DOJ）：是重大网络事件威胁响应行动的领导机构，通过 FBI 和国家网络调查联合特遣队（NCIJTF）开展工作。NCIJTF 由来自执法部门、情报共同体和国防部的 20 多家合作机构组成，是部门间协调、整合和分享网络威胁调查相关信息的关键节点。
- 国家情报总监办公室（ODNI）：是重大网络事件情报支持行动的领导机构，通过网络威胁情报整合中心（CTIIC）开展工作。CTIIC 提供态势感知、相关情报信息共享和威胁趋势及事件综合分析，并为跨机构的工作提供支持，以制定威胁缓解方案。CTIIC 还通过国家网络情报总监协调与事件相关的各项情报收集活动，包括确认情报差距。

根据联邦政府的资源和能力，联邦领导机构负责：

- 协调多机构的威胁或资产响应行动，以形成合力，包括协调任何可以为事件提供专业技术支持的机构和 SSA。
  - 根据情况，确保本机构负责的行动方向与其他网络 UCG 参与者和受影响实体的响应行动协调一致。
  - 根据需要，确认并向网络响应小组（CRG）推荐其他联邦政府资源或行动，以更好地对事件进行响应和恢复。
  - 围绕威胁、资产和受影响实体响应行动，通过网络 UCG 与受影响实体进行必要的协调。
- 除联邦领导机构以外，如果重大网络事件已经或可能影响 SSA 代表的部门或其他的联邦

---

① PPD-8 “国家战备”，2011 年 3 月 30 日签发，<https://www.dhs.gov/xlibrary/assets/presidential-policydirective-8-national-preparedness.pdf>。

网络安全中心，网络 UCG 在必要时也可将 SSA 纳入事件响应。参与重大网络事件响应的所有联邦机构均将参与网络 UCG，并与其协调响应行动。

当政府实体拥有或运营的关键基础设施受到或可能受到重大网络事件影响时，SLTT 政府将按要求参与网络 UCG。此外，网络 UCG 将按照现有的协作和信息共享机制，定期向 SLTT 合作伙伴提供更新。

像政府参与一样，只有那些对某具体事件的响应活动具有明显的责任、管辖权、职能或权限的私营部门才能参与网络 UCG，一般而言，不会包括所有对事件响应贡献了资源的组织。私营部门参与网络 UCG 是自愿的，其应有能力确定每个运行周期中的事件优先级，并能够批准“事件行动计划”，包括承诺其可以调动组织的资源来支持“事件行动计划”的实施。根据 PPD-41 的指导原则，联邦政府在保护受影响实体的隐私和敏感的私营部门信息的前提下，将采取广泛传播网络事件信息的方法协调受影响实体。随着特定事件响应情况的变化，网络 UCG 参与者的范围也将进行调整。

根据事件的性质和严重程度，网络 UCG 也可能会纳入特定的 ICT<sup>①</sup>公司（即 ICT 推动者），以直接协助具体事件的响应。如果某公司的功能和职能是全球网络生态系统的基础，那么这家公司就可被称为 ICT 推动者。这些处在信息分享有利位置的 ICT 推动者可以促进网络和 ICT 领域关键角色的积极参与，并为针对重大网络事件的大规模响应行动提供协助。

此外，网络 UCG 将继续利用现有的协调结构（如 SCC、ISAC 和日常运行呼叫）进行信息共享，以确保适当、及时地分享行动情报。作为很多关键基础设施部门的运行抓手，ISAC 可根据具体情况协助对本关键基础设施内部和跨基础设施的影响评估。其他组织可作为网络 UCG 成员，或作为联络组织，在不同的领导结构下与事件管理团队协作参与响应行动。通常，这些组织可对“事件行动计划”提出意见，但不对其内容或执行负责。

不管由哪类参与者组成，网络 UCG 的运行都应与保护情报和执法来源、方法、操作和调查的需求相一致，也要与保护个人隐私以及敏感私营部门信息的要求相一致。

#### （4）网络事件响应期间的信息共享

网络 UCG 应尽可能快速、公开、定期地与其他利益相关方共享事件响应过程中发现的网络威胁信息，以确保保护措施能够应用于所有适用的利益相关方。尽管这种信息共享有时受法律、法规、受影响实体的利益、涉密级别或安全要求以及其他操作考虑的限制，但在与利益相关方和公众共享信息时，参与者应尽力做到信息一致。此类信息一般通过现有的网络威胁信息共享渠道传播。

根据网络 UCG 参与者在特定事件中如何进行人员分配，信息共享有时也可通过网络 UCG 指定的公共信息官实施，或通过由参与响应的各组织的代表所组成的联合信息中心实施。在某些情况下，需要利用专门的信息共享机制向受影响的利益相关方提供有效的态势感知信息。在任何情况下，网络 UCG 都要以适宜方式保护个人隐私和敏感的私营部门信息。

---

① 详见总统国家安全远程通信顾问协会于 2014 年 5 月 21 日发布的《移动领域信息技术报告》，  
[https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%](https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%20)。

## 8. 结论

美国对加强网络技术的安全和韧性的努力从未停止。为了实现这种安全和韧性，公共-私营伙伴关系不可或缺，双方要共同确定优先事项、明确目标、降低风险，并根据网络事件的反馈和环境的变化不断适应和演进。联邦政府、SLTT 政府以及私营和国际合作伙伴仍将坚定地致力于保护网络、系统和应用程序，以应对当前和未来几十年可能面临的严峻网络风险。

DHS 网络安全和通信办公室将与 DOJ、ODNI 和各 SSA 协调，审查和维护 NCIRP，维护流程包括对行使职能所需的各项文件进行制定或更新。NCIRP 的重大更新将通过公共-私营高级审查程序进行审查。对本计划的审查将围绕以下目标进行：

- 评估和更新核心职能信息，以支持对网络事件以及网络、物理并发事件的响应目标。
- 确保该计划充分阐明了各负责实体的组织情况。
- 确保该计划符合国家战备目标的原则和事件保护、预防、减轻、应对和恢复的实践要求。
- 根据国家威胁或危害环境的变化更新各项流程。
- 将经验教训和有效做法纳入日常操作、演练、实际事件处理和警报中。
- 适应技术发展和变化带来的机遇和挑战。
- 反映国家网络事件响应行动的进展情况，说明执行新的法律、行政令和总统政策令的必要性，并说明国家优先事项和指南、关键任务或国家职能的战略性变化。

NCIRP 附录的增加或更新将通过基础文件审查独立进行，该基础文件包括从立法或法律变更、网络演习或现实世界事件中汲取的经验、教训。

## 附录 A 政策法规

下列法律法规和政策文件为联邦政府的并行响应活动（即威胁响应、资产响应和情报支持）提供了法律基础。另有其他法律和法规针对某些关键基础设施部门提出了进一步要求。

本附录并未列出所有相关法律法规，但可作为基础性的参考资料。

- 1934 年《通信法》第 706 条（公法 73-416）；
- 2015 年《网络安全法》（公法 114-113）；
- 1950 年《国防生产法》（公法 81-744）修正案；
- 第 12333 号行政令《美国情报活动》（EO-12333）修正案；
- 第 12382 号行政令《总统的国家安全电信咨询委员会》（EO-12382）修正案；
- 第 12829 号行政令《国家工业安全计划》（EO-12829）修正案；
- 第 12968 号行政令《涉密信息访问》（EO-12968）修正案；
- 第 13549 号行政令《针对州、地区、部落和私营部门实体的涉密国家安全信息计划》（EO-13549）；
- 第 13618 号行政令《国家安全任务和应急战备通信职能》（EO-13618）；
- 第 13636 号行政令《增强关键基础设施网络安全》（EO-13636）；
- 第 13691 号行政令《促进私营部门网络安全信息共享》（EO-13691）；
- 2014 年《联邦信息安全现代化法》（公法 113-283）；
- 2002 年《国土安全法》（经公法 112-265 修正）；

- 第 5 号国土安全总统令《国内事件管理》(HSPD-5);
- 2004 财年《情报授权法》(公法 108-177);
- 2004 年《情报改革和防范恐怖主义法》(公法 108-458);
- 2014 年《国家网络安全保护法》(公法 113-282);
- 2013 年国家基础设施保护计划《关于关键基础设施安全和韧性的伙伴关系》;
- 1947 年《国家安全法》(公法 80-253) 修正版;
- 第 42 号国家安全令《关于国家安全电信和信息系统安全的国家政策》;
- 第 54 号国家安全总统令/第 23 号国土安全总统令《网络安全政策》(NSPD-54/HSPD-23);
- 管理和预算办公室备忘录 M-07-16《针对侵害个人身份信息的安全防护和响应》;
- 第 8 号总统政策令《国家战备》(PPD-8);
- 第 21 号总统政策令《关键基础设施安全和韧性》(PPD-21);
- 第 25 号总统政策令《美国多边和平行动改革政策》(PPD-25);
- 第 40 号总统政策令《国家连续性政策》(PPD-40);
- 第 41 号总统政策令《美国网络事件协调》(PPD-41) 及其附件;
- 《美国法典(USC)第 6 编》: 国内安全;
- 《美国法典(USC)第 10 编》: 武装力量;
- 《美国法典(USC)第 18 编》: 犯罪活动和刑事诉讼程序;
- 《美国法典(USC)第 32 编》: 国民警卫队;
- 《美国法典(USC)第 47 编》: 电信;
- 《美国法典(USC)第 50 编》: 战争和国防。

## 附录 B 网络事件严重度图示

根据第 41 号总统政策令 (PPD-41)<sup>①</sup>, 在与联邦各部、局协调网络安全或网络运行行动时, 各联邦网络安全中心采用一个通用的图示来描述网络事件对美国国土安全、国家职能或国家利益造成影响的严重程度。该图示为评价和评估网络事件提供了一个通用框架, 确保所有的部、局对下列事项形成统一的观点:

- 特定网络事件的严重程度;
- 对特定网络事件进行响应的紧急程度;
- 协调响应工作所需的政府层级;
- 响应工作所需的资源投入等级。

下图描述了网络安全事件严重度图示的要素:

<sup>①</sup> <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>。

一般定义		观测到的行为	预期后果
5级 紧急 (黑)	对大范围关键基础设施服务的提供、国家政府稳定或美国人民生命安全构成紧迫威胁	见效	造成物理后果
4级 严重 (红)	很可能会对公众健康或安全、国家安全、经济安全、国际关系或公民自由造成重大影响		损坏计算机和网络硬件
3级 高级 (橙)	很可能会对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成明显影响		破坏或毁坏数据
2级 中级 (黄)	可能会对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成影响	实施	损害关键系统或服务的可用性
1级 低级 (绿)	不太可能对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成影响		窃取敏感信息
0级 基级 (白)	未经证实的或无足轻重的事件	接触	实施金融犯罪
		准备	引起轻微麻烦的拒绝服务攻击 (DoS) 或一般性破坏

附录 C 网络事件严重度图示和国家响应协调中心激活等级的对照

当事件影响到网络和（或）物理环境时，为做出最为适当的响应，某些决定和活动需要进行协调。下表对第 41 号总统政策令《美国网络事件协调》中给出的网络事件严重度图示和国土安全部国家响应协调中心激活等级进行了比较，以对比网络和物理事件的响应等级：

描 述	灾害等级	网络事件严重度	描 述	观测到的活动
由于其严重程度、影响范围、发生地点以及对公众健康、人民福祉和基础设施造成的实际或潜在影响，各级政府不具备对此类事件的响应能力，因此需要联邦为响应和恢复工作提供最大程度的协助	1 级	5 级 紧急	对大范围关键基础设施服务的提供、国家政府稳定、或美国人民生命安全构成紧迫威胁	结果
由于此类事件危害范围较大，严重程度中等，需要联邦和 SLTT 政府间的高级别协调。其中，FEMA 和其他联邦机构重点参与	2 级	4 级 严重	很可能会对公众健康或安全、国家安全、经济安全、国际关系或公民自由造成重大影响	存在
		3 级 高级	很可能会对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成明显影响	
由于此类事件危害范围和严重程度低于平均级别，需要联邦和 SLTT 政府间的一般协调。通常，此类事件的响应主要是事件恢复工作，仅包含最低程度的响应要求	3 级	2 级 中级	可能会对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成影响	预期
		1 级 低级	不太可能对公众健康或安全、国家安全、经济安全、国际关系、公民自由或公众信心造成影响	
无预期情况或事件。 本级别包括常规的监测预警活动	4 级	0 级	未经证实的或无足轻重的事件	稳定状态

## 附录 D 向联邦政府报告网络事件<sup>①</sup>

网络事件可能会造成严重的后果。针对个人隐私、财务或其他敏感数据的窃取和破坏计算机系统的网络事件能够对在线的私人或商业交易参与者造成持久的损害。企业、消费者和其他所有的互联网用户都面临着日益加剧的此类风险。

联邦政府部门已做好准备，以调查事件、协助缓解事件后果以及协助预防事件，为遭受网络事件影响的私营部门实体提供帮助。例如，联邦执法机构拥有众多受过高等训练、专门负责响应网络事件的调查员，他们可以阻止造成网络事件的威胁行为者并保护其他潜在受害者。

除执法机构之外，其他的联邦响应者能够为资产保护、脆弱性缓解提供技术支援，并能派出现场响应人员为事件恢复提供帮助。在支持受影响的实体时，联邦政府的各机构将协调合作，充分发挥各自专长，运用网络威胁知识协力响应，保护关键证据，并利用联合的权限和职能尽可能减少资产的脆弱性，使恶意行为者受到法律制裁。本附录说明了对于网络事件，应在何时以及如何向联邦政府报告。

### 1. 何时向联邦政府报告

网络事件是指，可能会损害数字信息或信息系统的保密性、完整性或可用性的事件。联邦政府重点关注那些能够造成重大危害的网络事件，因此，鼓励受害者报告所有可能产生下列后果的网络事件：

- 导致数据、系统可用性或系统控制措施的重大损失；
- 影响大量的受害者；
- 有迹象显示关键 IT 系统受到未经授权访问或存在恶意软件；
- 影响关键基础设施或核心政府职能；
- 影响国家安全、经济安全或公共卫生和安全。

2014 年《联邦信息安全现代化法》(FISMA) 要求，联邦行政部门民事机构应将有关其信息和信息系统（无论是由联邦机构、承包商还是其他机构管理）的信息安全事件通报给美国计算机应急准备小组 (US-CERT)，并就事件响应向 US-CERT 咨询。

### 2. 报告的内容

可以在网络事件发生的任何阶段（包括尚无法获取完整的事件信息时）向政府报告该事件。有效的报告应包含以下信息：事件报告者、事件受害者、发生事件的类型、事件最初被发现的时间和如何被发现、已经采取了哪些响应措施以及已经通知了哪些部门。

### 3. 如何向联邦政府报告网络事件

鼓励受网络事件影响的私营部门实体向联邦执法机构、该实体的对口联邦政府机构或下表中列出的任何联邦机构的地方办事处报告网络事件：

---

<sup>①</sup> 本文与第 41 号总统政策令“美国网络事件协调”一同编制，旨在向公众提供统一的联邦信息，说明为获得联邦政府的协助，应在何时以及如何报告网络事件，未提出任何法律法规或合同要求的强制报告义务。本文中要求的报告，应通过指定的联邦联络点并使用现有程序持续进行。

威胁响应	资产响应
<p>联邦调查局 (FBI)</p> <p>联邦调查局地方办事处网络工作小组: <a href="http://www.fbi.gov/contact-us/field">http://www.fbi.gov/contact-us/field</a></p> <ul style="list-style-type: none"> <li>➤ 网络犯罪投诉中心 (IC3): <a href="http://www.ic3.gov">http://www.ic3.gov</a></li> <li>➤ 向联邦调查局地方办事处网络工作小组报告网络犯罪, 包括计算机入侵或攻击、欺诈、知识产权盗窃、身份盗用、商业秘密窃取、黑客犯罪、恐怖活动、间谍活动、蓄意毁坏或其他外国情报活动</li> <li>➤ 向 IC3 报告个人网络犯罪事项, 受害人或第三方均可向 IC3 投诉网络犯罪</li> </ul>	<p>国家网络安全通信整合中心 (NCCIC) (888) 282-0870 或 <a href="mailto:NCCIC@hq.dhs.gov">NCCIC@hq.dhs.gov</a></p> <p>美国计算机应急准备小组 (US-CERT) <a href="http://www.us-cert.gov">http://www.us-cert.gov</a></p> <ul style="list-style-type: none"> <li>➤ 报告疑似的或已确认的网络事件, 包括受影响的实体希望得到联邦的协助, 以击退敌人、恢复运行和提出进一步改善安全的建议。</li> </ul>
<p>国家网络调查联合特遣队 (NCIJTF)</p> <p>CyWatch 7×24 小时指挥中心: <a href="mailto:cywatch@ic.fbi.gov">cywatch@ic.fbi.gov</a> 或 (855) 292-3937</p> <ul style="list-style-type: none"> <li>➤ 报告可能需要联邦执法机构或联邦政府的当地办事处行动、调查、参与的网络入侵和重大网络犯罪</li> </ul>	
<p>美国特勤局 (USSS)</p> <p>特勤局地方办事处和电子犯罪任务小组 (ECTF): <a href="http://www.secretservice.gov/contact/field-offices">http://www.secretservice.gov/contact/field-offices</a></p> <ul style="list-style-type: none"> <li>➤ 报告网络犯罪, 包括计算机入侵或攻击、传播恶意代码、贩卖密码、盗用支付卡或其他财务支付信息</li> </ul>	
<p>美国移民和海关执法局/国土安全调查局 (ICE/HSI)</p> <p>HIS 举报热线: 866-DHS-2-ICE (866-347-2423) 或 <a href="http://www.ice.gov/webform/hsi-tip-form">www.ice.gov/webform/hsi-tip-form</a></p> <p>HSI 地方办公室: <a href="https://www.ice.gov/contact/hsi">https://www.ice.gov/contact/hsi</a></p> <p>HSI 网络犯罪中心: <a href="https://www.ice.gov/cyber-crimes">https://www.ice.gov/cyber-crimes</a></p> <ul style="list-style-type: none"> <li>➤ 报告利用网络进行的犯罪, 包括: 对知识产权的数字盗窃; 非法电子商务 (包括地下市场); 利用互联网推动武器和战略技术扩散; 儿童色情; 利用网络进行的走私和洗钱</li> </ul>	

最初接到报告的联邦机构将与其他相关的联邦利益相关方协调响应事件。如果受影响的实体负有法律或合同规定的网络事件报告义务, 那么除了自愿将事件报告给相应的联邦联络点外, 该实体还应履行义务。鉴于网络事件的性质, 各联邦机构还应酌情与 SLTT 政府组织合作。

#### 4. 联邦事件响应的类型

收到网络事件报告后, 联邦政府将迅速集中力量开展两项活动, 即威胁响应和资产响应:

- 威胁响应: 包括溯源、跟踪和阻断恶意网络行为者和恶意网络活动。威胁响应行动包括实施刑事调查和抵制恶意网络活动的其他行动。
- 资产响应: 包括资产保护和降低对恶意网络活动的脆弱性。资产响应行动包括减轻对系统和 (或) 数据的影响; 加固、恢复和修复服务; 确定面临风险的其他实体; 评估更大范围内的潜在风险, 并缓解危及个人的潜在隐私风险。

无论事件类型或其响应方式如何, 联邦机构都会团结一致帮助受影响的实体了解事件、关



联相关事件并与其共享信息，从而在保护隐私和公民自由的基础上快速解决问题。

如果遇到直接威胁公共健康或安全的事件，公众应拨打报警电话（911）。

## 附录 E 联邦网络安全中心的角色

联邦政府已经建立了一些与各部、局相关联的网络安全中心，以执行运行任务、加强信息共享，维护对网络事件的态势感知，并作为公共-私营部门利益相关方实体之间的沟通渠道。为了支持联邦政府在网络事件管理方面的协调结构，网络统一协调小组（网络 UCG）<sup>①</sup>可以选择使用这些网络安全中心已制定的超过常备能力的增强性协调程序，和（或）运行或支持人员。

### 1. 国家网络安全通信整合中心（NCCIC）

作为国土安全部下属的运营单位，NCCIC 是协调联邦政府对网络事件进行资产响应的主要平台。NCCIC 的授权参见 2014 年《国家网络安全保护法》第 3 条。

### 2. 国家网络调查联合特遣队（NCIJTF）

NCIJTF 是一个多机构的中心，主办单位为联邦调查局。它是协调联邦政府威胁响应行动的主要平台。NCIJTF 由第 54 号国家安全总统指令/第 23 号国土安全总统指令第 31 项获准成立并授权。

### 3. 网络威胁情报整合中心（CTIIC）

CTIIC 由国家情报总监办公室负责运营，是联邦政府开展情报整合、分析和支持活动的主要平台。对于外国的网络威胁或影响美国国家利益的网络事件，CTIIC 还提供对所有来源情报的整合分析。

### 4. 美国网络司令部（USCYBERCOM）联合作战中心（JOC）

USCYBERCOM JOC 负责指挥美国军方的网络空间行动和保护国防部信息网络（DoDIN）。如网络事件影响到 DoDIN，USCYBERCOM 将在影响期间管理对 DoDIN 的威胁响应和资产响应，并根据需要获取其他中心的支持。

### 5. 国家安全局（NSA）网络安全威胁行动中心（NCTOC）

NSA 所属的网络安全威胁运行中心（NCTOC）是 NSA 全天候（7×24 小时×365 天）跟踪和评估外国网络安全威胁的机构。NCTOC 通过对外国情报的分析，向合作伙伴通报当前和潜在的恶意网络活动，重点包括敌对计算机网络攻击、攻击者能力和实施破坏途径等。NCTOC 也会根据要求向美国政府各部、局提供技术援助。

### 6. 国防部网络犯罪中心（DC3）

DC3 通过数字取证、重点威胁分析和培训来支持执法、反间谍、信息保障、网络防御和关键基础设施保护等活动。DC3 可提供分析和技术能力，协助联邦机构任务合作伙伴响应国家网络事件。

### 7. 情报共同体安全协调中心（IC-SCC）

IC-SCC 的任务是，根据国家情报总监首席信息官主任办公室的授权和指挥，联合各个情报共同体的任务合作伙伴对 IC 信息环境下的综合防御进行监控和监督。2014 年 IC SCC 成立后，IC 事件响应中心的角色和职责交由 IC SCC 执行。

<sup>①</sup> 网络 UCG 的描述参见本文第 7 章中“重大网络事件的运行协调”一节的第（3）小节。

## 附录 F 核心功能和关键任务

在“国家网络事件响应计划”（NCIRP）中，每项核心功能下都包含一些关键任务来促进功能的执行。这些任务是为了使各项功能达到理想的效果而必不可少的任务。关键任务可以使计划制定者在事件发生前明确资源分配和采购需求，从而推动达成任务目标。下表描述了各项核心功能及其关键任务：

<p>1. 访问控制和身份验证</p> <p>功能描述：采用并支持必要的物理、技术和网络措施来控制对关键位置和系统的准入，这也被称为鉴别和授权</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 验证身份，以授权、许可或拒绝对网络资产、网络、应用程序和系统的访问，防范其被利用和加以破坏。</li> <li>➤ 在授权用户进行合法活动时，控制和限制其对关键部位和系统的访问。</li> <li>➤ 坚持采取适当和必要的机制，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 开展审计工作，以核实和验证安全机制是否按照预期执行。</li> <li>➤ 开展培训工作，以确保所有员工遵守访问控制权限</li> </ul>
<p>2. 网络安全</p> <p>功能描述：保护（或必要时恢复）计算机网络、电子通信系统、信息和服务免受损坏、非授权使用和恶意利用。更多的时候，网络安全也被称为信息安全，它通过多项活动和工作来确保关键信息、记录、通信系统和服务的安全性、可靠性、保密性、完整性和可用性</p>
<p>3. 关键任务：</p> <ul style="list-style-type: none"> <li>➤ 落实对策、技术和政策，以保护可能被利用的物理和网络资产、网络、应用程序和系统。</li> <li>➤ 根据风险评估、风险缓解和事件响应功能的执行情况，分析资产的脆弱性，并基于此尽可能确保公共和私营网络及关键基础设施（如通信、金融、电子行业、水利和交通系统）的安全。</li> <li>➤ 构建支持基本功能持续运行且具有韧性的网络系统。</li> <li>➤ 坚持采取适当和必要的机制，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 尊重安全合作伙伴之间网络安全策略的限制和边界</li> </ul>
<p>4. 取证和溯源</p> <p>功能描述：针对事件的取证调查和溯源是重大网络事件中并行开展的互补功能</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 检索数字媒体和数据网络的安全和活动日志。</li> <li>➤ 进行数字证据分析，并遵守保管链规则。</li> <li>➤ 遵循必要的证据收集规则，进行物理证据收集和分析。</li> <li>➤ 评估可能的威胁行动者所拥有的能力。</li> <li>➤ 充分利用事件响应者的工作成果和对资产的技术溯源，来识别恶意网络行为者。</li> <li>➤ 如果可能，与证人、潜在有关人员或嫌疑人会面。</li> <li>➤ 在溯源任务中应用置信级别。</li> </ul>
<ul style="list-style-type: none"> <li>➤ 在溯源要素指南中，以共享产品为目的，将信息的内涵以及限制纳入其中。</li> <li>➤ 坚持采取适当和必要的机制，保护敏感和涉密信息，保护个人隐私、公民权利和公民自由。</li> </ul> <p>开展审计工作，以核实和验证安全机制是否按照预期执行</p>

续表

<p>基础设施系统</p> <p>功能描述：恶意网络活动发生后，要将关键基础设施功能稳定下来，减少对健康和安全的威胁，有效地响应和恢复系统和服务，以支持可靠、富有韧性的系统</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 保持对控制系统安全运行所需要的全面了解。</li> <li>➤ 保持基础设施稳定运行和恢复对其的控制。</li> <li>➤ 加大网络隔离的力度，以降低恶意网络活动广泛传播的风险，包括在企业内部或互联实体之间的传播。</li> <li>➤ 稳定可能受网络事件级联效应影响的实体内的基础设施。</li> <li>➤ 促进恢复和维持基本服务（包括公共和私营服务），以维护该行业的整体功能。</li> <li>➤ 坚持采取适当和必要的机制，以保护敏感和涉密信息，保护个人隐私、公民权利和公民自由。</li> <li>➤ 了解新兴和已有的可适用安全研究、产品和解决方案的最新数据和进展</li> </ul>
<p>5. 情报与信息共享</p> <p>功能描述：基于规划、指导、收集、开发、处理、分析、生产、传播、评估以及对针对美国及其人民、财产利益的恶意网络活动的反馈，提供及时、准确和可操作的信息。情报和信息共享是必要时在政府或私营部门实体之间交换情报、信息、数据或知识的功能</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 对于与网络脆弱性和威胁有关的运营环境变化，监控、分析和评估由其造成的积极和消极影响。</li> <li>➤ 通过参与伙伴之间的日常安全信息交流（包括威胁评估、警戒、威胁迹象、警告和预警）共享分析结果。</li> <li>➤ 确认网络安全利益相关方的情报和信息共享需求。</li> <li>➤ 为在私营部门与政府网络安全合作伙伴之间进行涉密情报和信息共享<sup>①</sup>，制定、明确访问机制和程序，并提供访问权限。</li> <li>➤ 使用情报流程来生产相关、及时、可访问和可操作的情报和信息产品并交付适宜的实体，以在本功能中纳入具有物理响应角色的关键基础设施参与者和合作伙伴。</li> <li>➤ 与 SLTT 实体、国际政府和私营部门共享可用的网络威胁信息，以促进态势感知共享。</li> <li>➤ 通过所有参与者均可访问的在线网络进行合作。</li> <li>➤ 坚持采取适当和必要的机制，保护敏感和涉密信息以及个人隐私、公民权利和公民自由</li> </ul>
<p>6. 拦截与阻断</p> <p>功能描述：延迟、转移、拦截、阻断、逮捕或保护与恶意网络活动相关的威胁</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 阻止美国境内、领地内和海外的恶意网络活动。</li> <li>➤ 阻止与潜在网络威胁或行为有关的人员。</li> <li>➤ 部署有关资产，拦截、阻止或阻断网络威胁损害潜在目标。</li> <li>➤ 利用执法和情报资源来识别、跟踪、调查和阻止威胁国家公共、私营信息系统安全的恶意行为者。</li> <li>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 尊重安全协作合作伙伴之间网络安全策略的限制和边界</li> </ul>

① 信息共享应为有访问或功能需求的个人提供有效沟通，其中，有访问或功能需求的个人包括不精通英语的或患有残疾（包括失聪、听力弱、失明或视力弱）的人。为有访问或功能需求的个人提供有效沟通包括使用适当的辅助性帮助或服务，如手语和其他翻译员、配有字幕的音频和视频材料、用户可访问的网站、使用多种语言进行沟通以及多元文化媒体。

续表

<p>7. 物流与供应链管理</p> <p>功能描述：促进和协助基本商品、设备和服务的交付，以支持受影响的系统和网络的响应。同步物流功能及恢复受影响的供应链</p> <p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 行动前，识别响应所需的资源并为其编制目录。</li> <li>➤ 调动和交付政府、非政府和私营部门的资源，以稳定事件、对响应和恢复工作进行，确保本功能包括对资源和服务的调拨与交付，以满足受事件影响的实体的需要。</li> <li>➤ 促进和帮助关键基础设施组件的交付，以快速响应并恢复网络系统。</li> <li>➤ 对受事件影响的关键基础设施实体，加强公共、私营资源和服务的支持。</li> <li>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 在上述所有关键任务中，应用供应链保障的原则和知识</li> </ul>
<p>8. 通信</p> <p>功能描述：采取一切可行手段，确保受影响实体和所有响应者之间进行及时通信，以支持安全、态势感知和运营</p> <p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 确保网络事件响应团体与受影响实体间的通信能力。</li> <li>➤ 在 SLTT（特别是州融合中心）、联邦和私营部门网络事件响应者之间建立可互操作的、冗余的语音、数据和其他更多的通信渠道。</li> <li>➤ 促进面向地方和地区建立可快速搭建的临时语音和数据网络，确保在网络服务中断的情况下，关键基础设施实体仍可协调响应行动。</li> <li>➤ 与为管理事件物理（或非网络）影响而成立的各 UCG（或实体）协调，确保能够根据具体情况提供安全可用的分布式、可扩展的事件响应通信功能，包括在传统通信或系统受损时，提供带外通信机制。</li> <li>➤ 坚持采取适当的措施，保护敏感和涉密信息，为促进快速信息共享，私营部门人员在通过安全审查后，应获得必要的许可和访问权限。</li> <li>➤ 保护个人隐私、公民权利和公民自由。</li> <li>➤ 网络威胁信息也可通过迹象信息自动共享措施，使用已建立的格式进行传播，如结构化威胁信息表达、可信的迹象信息自动交换 (STIX/TAXII)<sup>①</sup>。</li> <li>➤ 执行红色组行动，以验证和核实取证和溯源功能的执行符合预期并且具有足够的可见性</li> </ul>
<p>9. 运行协调</p> <p>功能描述：建立和维护统一、一致的运行结构和流程，适当地整合所有关键利益相关方，并支持核心功能的实施</p> <p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 在整个事件中，调动所有关键资源并建立必要的协调结构。</li> <li>➤ 在行动方案中，清晰定义各方的角色和职责并做好沟通。</li> <li>➤ 为确保协调一致，明确各项行动的优先顺序，并同步执行。</li> <li>➤ 确保实体在横向和纵向上均有明确的通信渠道和模式。</li> <li>➤ 根据 NIPP，确保相关的私营部门在网络事件响应全周期内参与到运行协调中。</li> <li>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 开展顶层设计活动，以验证和核实利益相关方之间协调的有效性、适当性</li> </ul>
<p>10. 规划</p> <p>功能描述：执行系统性的流程，使举国参与到制定可执行战略、操作或战术层面的方法上来，以实现既定目标</p>

① <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>。

续表

<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 基于现有计划，启动灵活的规划流程，并作为国家规划体系的一部分<sup>①</sup>。</li> <li>➤ 与合作伙伴协作，共同制定计划和流程，以促进事件响应行动的协调一致。</li> <li>➤ 建立伙伴关系，协调合作伙伴之间的信息共享，以便于恢复一个或多个司法管辖区和部门的关键基础设施。</li> <li>➤ 利用关键基础设施相互依赖性分析确定风险管理响应优先级。</li> <li>➤ 识别关键基础设施并区分其优先级，确定风险管理优先顺序。</li> <li>➤ 协同私营和非营利性部门以及地方、区域或大都市、州、部落、领地、岛屿地区、联邦的组织和机构，在不断变化的基础上，执行脆弱性评估，分析脆弱性及其可能造成的后果，识别能力差距并协调保护措施。</li> <li>➤ 基于规划需求，充明确关键目标，在联邦层面及各州、领地制定涵盖业务/服务影响分析、事件行动和事件支持的运行计划；提出一份完整的综合描述，说明为了达到目标，各任务升级和降级的顺序以及需要调整等级的任务的范围；确保在运行计划拟定的时间框架内，在可用的资源条件下，上述目标具备可执行性。</li> <li>➤ 以签署谅解备忘录或协商合同的形式，与政府和私营部门网络事件或应急响应小组之间建立正式的合作伙伴关系，从而有效接受、鉴别和协作响应网络事件。</li> <li>➤ 在负责网络安全、负责依赖网络安全的物理系统的团体和学科间建立正式的合作伙伴关系。以签署谅解备忘录或协商合同的形式，在 ICT 和信息系统供应商及其客户之间就当前产品网络安全、业务规划以及必要时的响应和恢复，建立正式的合作伙伴关系。</li> <li>➤ 与政府和私营部门实体建立正式的合作伙伴关系，在事件的事前、事中和事后，共享数据和威胁情报。</li> <li>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由</li> </ul>
<p>11. 公共信息和警告</p> <p>功能描述：采取清晰、一致、可访问的、符合文化和语言习惯的方法，适时向全国和公众发布统一、及时、可靠并可操作的信息，旨在有效传播关于重大威胁或恶意网络活动的信息，或是正在采取行动和提供援助的相关信息</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 建立可用的机制，并提供所需的全方位支持，以在各级政府、私营部门、宗教组织、非政府组织和公众间开展适当的、持续的信息共享。</li> <li>➤ 与公共、私营和非营利部门以及各级政府共享可用的信息，并向它们提供态势感知。</li> <li>➤ 采取一切可行的通信手段，如整合的公众警报和预警系统、公共媒体和社会媒体网站。</li> <li>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</li> <li>➤ 尊重可适用的信息共享和隐私保护要求，包括“交通灯协议”。</li> <li>➤ 保障还有冗余选项可用，以实现关键的公共信息、威胁指示和预警信息的传播</li> </ul>
<p>12. 筛选、搜索和检测</p> <p>功能描述：通过主动和被动的监视及搜索程序来识别、发现或定位恶意网络活动的威胁，包括采取系统性检查和评估、传感器技术或物理调查和情报等方法</p>
<p>关键任务：</p> <ul style="list-style-type: none"> <li>➤ 定位与网络威胁有关的人员和网络。</li> <li>➤ 与关键基础设施参与者（私营行业和 SLTT 合作伙伴）建立关系并推动其进一步参与。</li> <li>➤ 开展符合法律授权的物理和电子搜索。</li> </ul>

① 国家规划体系提供了统一的方法和通用的术语，通过一些规划支撑国家战备体系的实施，这些规划支持以一种“所有威胁和危害”的方法进行战备。这些规划（包括战略性的、操作性的还有战术性的）将确保整个团体协调一致地建立、维护和交付国家战备目标中明确的核心功能。

续表

<div>➤ 收集和分析提供的信息。</div> <div>➤ 检测和分析恶意网络活动，并支持威胁缓解活动。</div> <div>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</div> <div>尊重安全协作合作伙伴之间网络安全策略的限制和边界</div>
<div>13. 态势评估</div> <div>功能描述：向所有决策者及时提供恶意网络活动的性质和范围、级联效应以及响应状态的决策信息</div>
<div>关键任务：</div> <div>➤ 协调建模及其效果分析的生成和传播，以用于网络事件即时响应行动。</div> <div>➤ 维护标准报告模板、信息管理系统、信息基本要素和关键信息需求。</div> <div>➤ 制定一套通用的操作流程，用于在两个及以上的组织间共享相关事件信息。</div> <div>➤ 协调多源信息的结构化收集和获取，以便将其纳入评估流程。</div> <div>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由</div>
<div>14. 威胁和危害识别</div> <div>功能描述：识别影响网络和系统的恶意网络活动威胁，确定这些威胁的频率和量级，并将其纳入分析和规划流程，以便清楚地了解各实体的需求</div>
<div>关键任务：</div> <div>➤ 识别各利益相关方的数据需求。</div> <div>➤ 及时有效地生成和收集所需数据，以准确识别网络威胁。</div> <div>➤ 确保适当的人员在适当的时间接收到适当的数据。</div> <div>➤ 通过适当的分析和收集工具将数据转化为有意义和可操作的信息，供公众使用。</div> <div>➤ 坚持采取适当和必要的措施，保护敏感和涉密信息以及个人隐私、公民权利和公民自由。</div> <div>➤ 发现、评估和解决政策上的差距，促进或实现技术、伙伴关系和程序，以解决妨碍各部门有效识别威胁、脆弱性和危害的问题</div>

附录 G 制定内部网络事件响应计划

本附录描述了制定网络事件响应计划的流程。第一部分描述了国家运行计划流程；第二部分概述了各实体可采用的计划流程。

国家运行计划

运行计划是为了达到预期目标而采取的连续的、不断完善的手段，可以最大程度地利用机会，指导响应活动。运行计划是“灵活的文件”，需要随着事件的发展和新信息的出现不断修订。运行计划旨在：

- 增强协调、协作和沟通，根据网络事件不同的严重程度，确定相应的行动计划和阶段性措施，并进行优先排序。
- 提高收集、分析多源信息及处理其中相冲突信息的能力，以实现及时、可执行的态势感知。
- 向广泛的利益相关方发出警报和警告，以提高防范意识，并启动事件响应行动、事件后果管理和业务连续性计划。
- 通过说明和明确各方的角色和职责，减少可能会对有效协调造成影响的冗余和重复。
- 通过增强可预测性和可持续性来提高协作水平，为管理事件后果、评估并减轻影响提

供保障。

- 增强灵活性和敏捷性，以更好地应对新事件和活动。

运行计划是各级政府和私营部门的固有职责，具有广泛的实施范围。应定期开展运行计划演练，以便明确差距，并制定持续的改进计划，从而提升针对网络事件的信息共享流程的有效性和战备水平。

NCIRP 不是网络事件响应的具体操作计划，而是各利益相关方制定本机构、本组织的运行计划时，应遵循的主要战略方针。作为通用的准则，NCIRP 将促进各项应急运行计划协调一致，并帮助受网络事件影响的机构了解联邦各部、局和其他的国家级合作伙伴如何为 SLTT 和私营部门响应行动提供资源支持。

### 响应运行计划

各机构和组织可以将“综合战备指南”(CPG) 101<sup>①</sup>和“响应联邦机构间运行计划”(响应 FIOP)<sup>②</sup>作为基础文件直接引用或针对网络事件进行裁剪，以制定本机构的响应运行计划。

CPG 101 提供了各种类型计划的信息和计划中各项基础的指南。根据 CPG 101，制定针对事件的联邦计划可使用以下的六步流程：

- 组建协作计划小组；
- 了解情况；
- 确定目的和目标；
- 制定计划；
- 准备、审查和批准计划；
- 落实和维护计划。

“响应 FIOP”则概述了联邦政府如何交付核心响应功能。它给出了关于角色和职责的信息，确定了各实体执行核心功能时的关键任务，明确了资源、采购的需求。响应 FIOP 在整个计划的运行概念中描述了与其他任务域的互依赖与整合，也描述了对并行活动和协调重点的管理，包括网络事件的预防、防护、减缓和恢复。响应 FIOP 不包括对具体部、局功能的详述，此类信息参见部级或局级的运行计划。

NRF 和 NIMS 可指导对响应 FIOP 的制定。NRF 基于分级响应的概念，认为绝大多数事件开始于地方级或部落级，随着响应需求超出该级别响应实体的资源和能力范围，逐步纳入其他的 SLTT 和联邦资产来应对网络事件。因此，响应 FIOP 应与其他 SLTT、岛屿区域和联邦的计划保持一致，以确保所有响应合作伙伴具有相同的行动重点。类似地，整合发生在联邦层面，各部、局和非政府合作伙伴通过 NRF、各实体的 FIOP、部和局的运行计划，整合形成各自的任务域。

### 应用

虽然 NRF 没有对行动的其他响应要素提供指导，但 NRF 和响应 FIOP 包含的指南能够帮助 SLTT、岛屿区域政府、非政府组织和私营部门了解联邦政府如何对事件做出响应。这些合作伙伴可以利用相关指南来完善它们的计划，确保准确了解联邦能够提供的援助和响应，以及提供支持的方式。

<sup>①</sup> CPG 101,“制定和维护应急运行计划”(第二版),2010年11月,<https://www.fema.gov/media-library/assets/documents/25975>。

<sup>②</sup> “响应联邦机构间运行计划”(第二版),2016年8月,[https://www.fema.gov/media-library-data/1471452095112\\_-507e23ad4d85449ff131c2b025743101/Response\\_FIOP\\_2nd.pdf](https://www.fema.gov/media-library-data/1471452095112_-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf)。

## 制定内部网络事件响应计划

公共-私营部门实体应考虑制定各自的网络事件响应运行计划，以进一步组织和协调针对网络事件的响应工作，各组织制定的计划应能满足本组织的独特需求，符合组织的使命、规模、结构和功能。

NIST SP 800-61（第2版）<sup>①</sup>概述了在制定网络事件响应计划时应考虑的若干要素。在制定计划时，各组织应根据自身需求进行裁剪、明确优先顺序，并遵守现有的信息共享和报告要求、准则和程序。鼓励公共-私营部门实体协作，共同制定网络事件响应计划，以促进态势感知和信息的共享，并了解互相之间在部门、技术和地理位置上的依赖关系。

制定网络事件响应计划需要一些重要的准则，下面列举的要素可以作为建立准则的基础：

- 使命；
- 战略和目标；
- 事件响应的组织方法；
- 风险评估；
- 网络事件评分系统/标准<sup>②</sup>；
- 事件报告和处理要求；
- 事件响应小组如何与组织内其他成员或其他组织进行沟通；
- 衡量事件响应功能及其有效性的指标；
- 使事件响应功能更加成熟的路线图；
- 计划如何与整个组织相适应；
- 与外部伙伴进行沟通，例如：
  - 客户、委托人和媒体；
  - 软件和支持的供应商；
  - 执法机构；
  - 事件响应者；
  - 网络服务提供者；
  - 关键基础设施部门合作伙伴。
- 角色和职责（准备、响应和恢复）：
  - 州融合中心；
  - 应急运营中心；
  - 地方、区域、州、部落和领地政府；
  - 私营部门；
  - 普通公民。
- 培训和演练计划，用于与响应团体协调资源分配；
- 对该计划进行维护的进度和程序。

---

① NIST SP 800-61（第2版），计算机事故处理指南，2012年8月，<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>。

② NCCIC 网络事件评分系统可作为基础，帮助组织运营中心对具体事件进行内部评估，<https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>。



附录 H 核心功能、NIST 网络安全框架和 PPD-41 的对照

NCIRP 对照表描述了 NCIRP 与 NIST 网络安全框架、PPD-41 之间的关系。在对照表中，各个核心功能被交叉引用，以确保三个文件之间的连续性和衔接。应以该表为基础，促进 NCIRP 各核心功能下的响应活动，了解 NIST 网络安全框架的功能和分类，以及 PPD-41 相应的并行工作线：

NCIRP 核心	核心功能	NIST 网络安全框架功能和分类				PPD-41 并行 工作方向
		识别	防护	检测	响应	恢复
访问控制	采用并支持必要的物理、技术和网络措施来控制对关键位置和系统的准入		访问控制 防护技术			
网络安全	保护（必要时也包括恢复）计算机网络、电子通信系统、信息和服务免受损坏、未授权使用和恶意利用	资产管理 业务环境 风险评估 风险管理战略	访问控制 数据安全 信息保护流程和程序 防护技术	异常现象和事件 持续安全监控 检测流程	沟通 响应计划 分析 缓解	沟通 改进 恢复计划
取证和溯源	针对事件的取证调查和溯源是重大网络事件中并行的互补功能				分析	
基础设施系统	恶意网络活动发生后，要将关键基础设施功能稳定下来，减少对健康和安全的威胁，有效地响应和恢复系统和服务，以支持可靠、富有韧性的系统	资产管理 业务环境 风险评估	访问控制 数据安全 信息保护流程和程序 防护技术	异常现象和事件 持续安全监控 检测流程		沟通 改进 恢复计划
情报与信息共享	基于规划、指导、收集、开发、处理、分析、生产、传播、评估以及对针对美国及其人民、财产或利益的恶意网络活动的反馈，提供及时、准确和可操作的信息。情报和信息共享是必要时在政府或私营部门实体之间交换情报、信息、数据或知识的能力	资产管理 业务环境	意识和培训 数据安全	持续安全监控 检测流程	沟通 分析 缓解 改进	沟通
拦截和阻断	延迟、转移、拦截、阻断、逮捕或防护与恶意网络活动相关的威胁					
						威胁响应 资产响应 情报支持
						威胁响应

续表

NCIRP 核心	核心功能	NIST 网络安全框架功能和分类					PPD-41 并行 工作方向
		识别	防护	检测	响应	恢复	
物流与供应链 管理	促进和协助基本商品、设备和服务的交付，以支持受影响的系统和网络的响应，包括同步物流功能及受影响供应链的恢复	业务环境					资产响应
通信	采取一切可行手段，确保受影响实体和所有响应者之间进行及时通信，以支持安全、态势感知和运营	资产管理		沟通	沟通		威胁响应 资产响应 情报支持
运行协调	建立和维护统一的、一致的运行结构和流程，整合所有关键利益相关方，并支持核心功能的实施	治理 风险评估 风险管理	异常现象和事件				威胁响应 资产响应 情报支持
规划	执行系统性的流程，使举国参与制定可执行战略、操作或战术层面的方法，以实现既定目标				响应计划	恢复计划 改进	威胁响应 资产响应 情报支持
公共信 息和预警	采取清晰、一致、可访问的、符合文化和语言习惯的方法，适时向全国和公众发布统一、及时、可靠并可操作的信息，旨在有效传播关于重大威胁或恶意网络活动的信息，或是在正在采取行动和提供援助的相关信息				沟通	沟通	威胁响应 资产响应 情报支持
筛选、搜 索和检测	通过主动和被动的监视及搜索程序来识别、发现或定位恶意网络活动的威胁			异常现象和事件 持续安全监控 检测流程			威胁响应 资产响应 情报支持
态势评估	向所有决策者及时提供恶意网络活动的性质和范围、级联效应以及响应状态的决策信息。 针对网络事件，该功能聚焦于快速处理和传达从国家层面到现场层面收到的大量信息，为所有决策者提供最新和最准确的信息	业务环境 沟通 意识和培训		检测流程	沟通	沟通	威胁响应 资产响应 情报支持
威胁和危 害识别	识别影响网络和系统的恶意网络活动威胁，确定这些威胁的频率和量级，并将其纳入分析和规划流程，以便清楚地了解各实体的需求			异常现象和事件 持续安全监控 检测流程			威胁响应

## 附录 I 其他资源

以下列举了私营-公共部门可以利用的其他资源。各实体可将本附录作为基础资料，了解网络事件响应、漏洞更新、数据泄露信息、风险管理和作为公共-私营部门联络点的组织等信息。这个并非一网打尽的列表以机构的英文首字母排序，提供了宽泛的信息，也可为本文件范围之外的用途提供参考。

- 网络安全中心（CIS）：[www.cisecurity.org](http://www.cisecurity.org);
- CIS 关键控制措施：<https://www.cisecurity.org/critical-controls.cfm>;
- 网络事件严重度图示：
- <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>;
- DHS 关键基础设施网络团体自愿计划：<https://www.us-cert.gov/ccubedvp>;
- 政府协调委员会：<https://www.dhs.gov/gcc>;
- 信息共享和分析组织：<https://www.isao.org>;
- 基础防护（Infragard）：[www.infragard.org](http://www.infragard.org);
- 工业控制系统安全计算机应急响应小组：<https://ics-cert.us-cert.gov>;
- 恶意软件调查员：<https://www.malwareinvestigator.gov>;
- MITRE 常见脆弱性和披露：<https://cve.mitre.org>;
- 州际信息共享和分析中心（MS-ISAC）：<http://www.nationalisacs.org>;
- 信息共享和分析中心全国委员会：<http://www.nationalisacs.org>;
- 国家事件管理体系：<https://www.fema.gov/national-incident-management-system>;
- 国家脆弱性数据库：<https://nvd.nist.gov>;
- NIST 增强关键基础设施网络安全框架：<https://www.nist.gov/cyberframework>;
- NIST 国家清单项目资源库：<https://web.nvd.nist.gov/view/ncp/repository>;
- NIST SP 800-61 “计算机事件处理指南”（第 2 版）：  
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>;
- NIST SP 800-37 “在联邦信息系统中应用风险管理框架指南”：<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>;
- NVD 通用脆弱性评分系统：<https://nvd.nist.gov/cvss.cfm>;
- 部门协调理事会：<https://www.dhs.gov/scc>;
- 美国计算机应急准备小组（US-CERT）网站：[www.us-cert.gov](http://www.us-cert.gov)。

---

## 三十二、“国家网络安全促进委员会” 报告（节选）

国家网络安全促进委员会<sup>①</sup>

2016 年 12 月

---

---

<sup>①</sup> 该委员会由《国家网络安全行动计划》所设立，美国前总统奥巴马在卸任前指示该委员会制定了此报告，提出了对今后美国网络安全的行动建议，是奥巴马留给特朗普的“政治遗产”。——译者注

## 摘要

由于认识到互联技术为数字经济带来的巨大收益，同时也注意到随之而来的网络环境安全威胁所形成的挑战，奥巴马总统建立了“国家网络安全促进委员会”（以下简称“委员会”）。总统指示，委员会要评估美国国家网络安全状态。总统还要求委员会为保护数字经济安全提出可操作的建议。总统要求，在实现加强网络安全的目标的同时，要保护个人隐私，确保公共安全、经济安全和国家安全，并促进新技术解决方案的发现和发展。

互联网和更广泛的数字生态系统带来的互联性和开放性，为社会创造了巨大价值，但这也同样使得保护网络环境安全变得更加困难。随着世界越来越融入和依赖信息革命，入侵、破坏、操纵和盗窃的速度也在加快。如果我们不改变实施和实现网络安全的战略及实践措施，技术进步将不断超越安全防护能力，并且这种局面还将持续存在。消费者的设备每天都要因恶意使用而遭受破坏。这些网络攻击事件充分表明，我们生活在一个越来越互相依赖的世界，关键基础设施与其他设施之间曾经泾渭分明，如今这个分界线变得越来越模糊。

威胁是现实存在的，我们必须保持一个平衡的视角，在创新、易用和安全之间寻求折中。互联网是社会变革和经济繁荣最有力的引擎之一。我们需要充分利用互联网的这些特性，同时加强其保护，使得其能够对抗攻击和滥用。为了应对这些问题，我们必须以过去几年私营部门和政府部门的安全工作为基础，改变现有网络安全防护策略、技术和最佳实践。

网络安全方面的投入要与技术创新相匹配。数字经济要实现繁荣发展，其必须是安全的。这就意味着社会中每个参与者，无论大公司还是小公司、各级政府部门、教育机构还是个人，都必须主动、积极应对网络风险。他们必须为其自己的安全承担更大的责任和义务，众所周知，这将直接影响我们国家的网络安全。

委员会成立以来，为奥巴马总统和即将上任的总统编制了一份报告。委员会委员具有丰富的网络安全相关知识，审阅了以往的报告，并与技术和政策方面的专家进行了深入沟通交流。委员会召开了多场公开听证会，吸收了各方面的信息输入，并尽可能邀请公众提供建议和案例。报告编制过程主要关注关键基础设施、物联网、研发、公共意识和教育、治理、人才、州和地方政府事务、身份管理和鉴别、保险、国际问题以及中小企业的角色等领域。

委员会考虑并确定了可能更广泛地影响上述主题的趋势，特别是：信息技术与物理系统的融合；风险管理；隐私与信任；全球和国家的影响力与控制力；自由市场和监管体系及解决方案的有效性；法律与责任的考虑；开发有意义的网络安全衡量标准的重要性和困难程度；基于自动化技术的网络安全方法；消费者责任等。在这些领域，委员会委员研究了什么是有效的机制，什么是主要挑战，以及如何去激发和培养公共-私营部门的网络安全文化。

有很多方面需要达成一致，包括：互联世界的不断融合和互依赖性；需要有更好的意识、教育和利益相关方在网络安全各方面的积极参与，从开发商、服务提供商到政策制定者和消费者；中小企业在处理网络安全问题时如何面对压力和有关限制，以及解决这种困境的重要性，尤其是考虑到它们在供应链中的作用时；从运行和任务的角度，如何明确联邦政府的角色和责任。

很明显，大多数解决方案需要公共-私营部门的共同努力。社会上每个参与者，无论是大公司和小公司、各级政府部门、教育机构还是个人，都必须主动、积极地应对网络风险。他们必须理解其在保护其自身网络安全时的角色，以及他们的行为如何更广泛地直接影响到国家的

网络安全。

其他更多需要考虑的领域有：

- 如何更好地激励网络安全行为和活动，以及如何确定是否或什么时候需要提出安全需求。
- 谁应牵头制定最急需的标准，以及如何更好地评价这些标准是否得到落实。
- 最可行的告知消费者的方式是什么，如通过标记技术和分级系统。
- 最需要的是何种研发方式以及研发的成本。
- 如何正确规划经济发展所需的新一代网络安全专家数量，以及如何选择吸收和培养不同级别人才队伍的方法。
- 高层联邦官员应承担何种角色？各官员之间是什么关系？如何确保这些官员不仅具有合适的授权，而且有权采取适当行动？

通过以上讨论，可以得出一些肯定性结论。国家之间、国家政府与州政府之间、各级政府机构与私营部门之间的合作，是鼓励技术、政策和措施得到应用的有力工具，以保护和促进数字经济增长。委员会认为，必须加强公共-私营部门间在网络安全事件的事前、事中、事后的合作。任何组织不可能单独解决网络安全问题。

韧性是任何网络安全战略的一个核心组成部分，因为当今动态的网络威胁环境需要通过风险管理方法予以迅速响应攻击，并能够快速恢复。

在建立共识和确定基本原则后，委员会委员将报告成果整理成 6 个主要要求，包括 16 项建议和 53 条行动措施。6 个要求如下：

- (1) 保护、防御当今信息基础设施和数字网络并确保其安全。
- (2) 创新数字网络和数字经济的安全与发展，并加大投资。
- (3) 使消费者在数字时代生活得更好。
- (4) 打造网络安全人才队伍能力。
- (5) 使政府职能在数字时代得到更有效和更安全的运转。
- (6) 确保开放、公平、竞争和安全的全球数字经济发展。

附录 A 详细描述了上述 6 个要求以及相应的建议和行动措施。附录中的分类不是孤立、割裂的。相反，很多建议可能适用于多个要求，它们仅仅是被编排在第一次出现的要求之中而已。这些文字也注明了在什么情况下行动措施与其他要求特别具有相关性。附录中的分类结构恰恰反映了数字经济相互依赖的本质。在这个时代，用来改进一个企业的网络安全的措施，能够有效地提升其他企业的安全态势与成熟度。

每条建议都会产生显著影响，相应的每项行动措施都是为取得该影响而采取的具体步骤。很多措施需要的财务资源远超过我们今天的预见。有些建议可能指向政府、私营部门，或者同时指向两者。有些建议需要全新的项目支持，有些可以依赖于现有项目得到解决。

鉴于国家面临挑战的紧迫性，委员会认为大多数建议能够而且也应该在近期开始实施，下届政府应在执政的前 100 天内启动计划。所有建议和行动措施都强调了一个事实，即私营部门、政府和美国公众应认识到，网络安全是我们国家繁荣昌盛的组成部分，将影响国家安全和经济安全，关系到我们对保持自由开放社会的期望。

## 附录 A 要求、建议和行动措施

### 要求 1：保护、防御当今信息基础设施和数字网络并确保其安全

建议 1.1	私营部门和政府应加强合作，建立提高数字网络安全的路线图，尤其是通过建设富有韧性的网络，抵御针对用户和国家网络基础设施的拒绝服务、欺骗以及其他类型的攻击
行动措施 1.1.1	总统应指示联邦高级行政官员启动一项公共-私营合作计划，针对用户和国家网络基础设施受到的攻击，建立灵活的、协调的攻击响应和缓解机制，在公共-私营合作计划中应落实、监测、跟踪和报告相关进展（短期）
建议 1.2	随着网络与物理世界的日益融合，联邦政府应与私营部门紧密合作，定义和建立保护基础设施的新模型
行动措施 1.2.1	总统应通过行政令，建立“国家网络安全公共-私营合作项目”（NCP），将作为处理网络安全事务的一种高级、联合的公共-私营合作平台（短期）
行动措施 1.2.2	私营部门和联邦政府应启动一个联合网络安全运行项目，用于促进公共-私营部门合作，共同开展网络安全活动，从而对影响关键基础设施的网络事件进行识别、保护、检测、响应和恢复（中期）
行动措施 1.2.3	联邦政府应为公司提供主动、直接参与正式政府合作的机会，共同推进网络风险管理实践，建立基于“网络安全框架”的联合防御计划（短期）
行动措施 1.2.4	联邦机构应对现有信息共享战略的实施作进一步扩展，包括交换网络供应链中关于组织互依赖性的信息（短期）
行动措施 1.2.5	随着所有组织间无线网络通信的增多，以及国家对全球定位系统（GPS）依赖性（用于定位、航海和定时）的提高，网络安全战略必须覆盖电磁频谱中的各种风险。当前目标是提高国家检测和解决故意的无线破坏的能力，提高无线通信和定时数据的韧性和可靠性（短期）
建议 1.3	下届政府应启动一个国家层面的公共-私营合作项目，推动对强鉴别技术的应用，以改进身份管理，从而使安全和隐私管理明显改观
行动措施 1.3.1	下届政府应要求，所有提供给公民的基于互联网的联邦政府服务都要强制使用适宜的强鉴别技术（短期）
行动措施 1.3.2	下届政府应指示，所有联邦机构必须使用强鉴别技术，包括其雇员、合同商以及其他任何使用联邦系统的人（短期）
行动措施 1.3.3	政府应当作为身份属性的认证源，以解决在线身份问题（中期）
行动措施 1.3.4	下届政府应成立一个由公共-私营部门组成的专家组，对设备和过程提出身份管理要求，以支持对数据源的规范（短期）
建议 1.4	下届政府应充分利用“网络安全框架”的成功经验，积极维持和提高该框架的使用，从而降低关键基础设施内外部的安全风险
行动措施 1.4.1	美国国家标准与技术研究院（NIST）应与 NCP 合作成立一个“网络安全框架评估标准工作组”（CFMWG），制定行业领先且一致认可的评估标准，供以下方面使用：（1）工业界用来自愿评估其公司的风险；（2）财政部和保险公司用来理解是否需要把安全纳入保险覆盖范围，以及如何使保险费用做到标准化；（3）美国国土安全部用来建立全国范围的自愿性网络安全事件报告项目，以确定网络安全的不足。这一报告项目应将网络事件数据和分析库包含在内（短期）
行动措施 1.4.2	所有联邦机构应使用“网络安全框架”（短期）

续表

行动措施 1.4.3	监管机构应将现有和将要制定的监管规定与“网络安全框架”相协调，侧重点是风险管理——降低违规守法的成本，并修改那些无助于网络安全甚至有意压制而不是鼓励创新的监管规定（短期）
行动措施 1.4.4	私营部门应开展有效、高效的合格评定项目，支撑美国公司的国际贸易和商务活动（短期）
行动措施 1.4.5	政府应将进一步的激励措施投向那些实施了网络风险管理原则且展现了合作成效的公司（短期）
建议 1.5	下届政府应开展具体工作，支持和加强中小企业网络安全
行动措施 1.5.1	NIST 应加强对中小企业在使用“网络安全框架”的支持，并评估其对中小企业的性价比（短期）
行动措施 1.5.2	经与私营部门合作，DHS 和 NIST 应通过国家网络安全卓越中心（NCCoE），制定如何集成和使用现有网络安全技术的蓝图，侧重点是如何满足中小企业的需求（短期）
行动措施 1.5.3	关键基础设施部门对口的政府机构（SSA）、行业协会和组织应合作启动一个项目，评估以往对公共网络的攻击，吸取这些安全事件的经验教训，包括关注中小企业如何利用这些经验教训（短期）

## 要求 2：创新数字网络和数字经济的安全与发展，并加大投资

建议 2.1	联邦政府和私营部门合作伙伴必须快速、积极地开展合作，提高物联网（IoT）的安全
行动措施 2.1.1	为了促进安全的物联网设备和系统的发展，总统应在 60 天内签发行政令，指示 NIST 与产业界及自愿性标准化组织合作，确定从关键系统到消费者/商业应用方面的已有标准、最佳实践以及部署差距等，且尽快就建立一套基于风险管理的安全标准集达成一致，需要时制定新标准（短期）
行动措施 2.1.2	监管机构应评估，“行动措施 2.1.1”中确定的网络安全实践措施和技术是否得到了及时、有效的实施，以增强网络安全。如果存在差距，应制定任何适宜的规则予以应对（中期）
行动措施 2.1.3	美国司法部应与商务部、国土安全部开展跨部门的研究项目，并与联邦贸易委员会、消费者产品安全委员会以及感兴趣的私营部门团体合作，就如何对错误 IoT 设备引发破坏的责任进行认定，在 180 天启动对现有法律的评估，并给出相关建议（短期）
行动措施 2.1.4	工业控制系统网络应急响应小组（ICS-CERT）应制定和传播物联网安全指南，以及与隐私有关的最佳实践，这些指南和最佳实践应易于部署和使用（短期）
建议 2.2	联邦政府应把可用、经济、本质安全的、防御性的、富有韧性/可恢复的系统作为优先发展的网络安全研发项目
行动措施 2.2.1	科技政策办公室主任应牵头制定一份公共-私营部门网络安全路线图，用于研发可用、经济、本质安全的、富有韧性/可恢复的、能保护隐私的、可操作性强的、防御性的系统。总统预算申请中所增加的主要研发基金应对此予以支持（短期）
行动措施 2.2.2	美国政府应支持将网络安全相关研究的精力投入以往获得支持资金较少的领域，包括人力资源因素和可用性，政策、法律、衡量标准，隐私和安全技术的社会影响，以及针对中小企业的特定问题等。在这些领域，通过研究可以提供切实可行的解决方案（短期）

## 要求 3：使消费者在数字时代生活得更好

建议 3.1	信息技术与通信部门的企业领导需要与消费者组织和联邦贸易委员会合作，为消费者提供更好的信息，以帮助他们在购买和使用互联产品和服务时做出正确的决定
行动措施 3.1.1	为了帮助消费者做出正确的购买决定，需要一个独立的组织为互联技术产品和服务制定一个网络安全“营养成分标签”。理想状态下，其应为一个易理解的、公正的、第三方评估的分级系统相关联，这样可以帮助消费者更直观采信和理解（短期和中期）
行动措施 3.1.2	下届政府执政后的 100 天内，白宫应召集一个有商业、教育、消费者和各级政府领导参与的峰会，对启动一个旨在提高国家网络安全意识和参与度的项目进行规划（短期）
行动措施 3.1.3	联邦贸易委员会应召集消费者组织及工业界的利益相关方启动一项目，制定标准文档模板，以告知消费者作为公民在数字经济中应承担的网络安全角色和责任，并制定《数字时代消费者权力和责任法》（中期）



续表

建议 3.2	联邦政府应建立、加强和扩展研发项目方面的投资，通过更好地理解人类行为及其与物联网和其他互联技术的互动，提升消费者产品和数字技术的网络安全及可用性
行动措施 3.2.1	根据 2016 年联邦网络安全研发战略计划，下届政府和国会应优先支持与人类行为和网络安全相关的项目（短期）

## 要求 4：打造网络安全人才队伍能力

建议 4.1	国家应通过人才能力建设积极应对人才队伍缺口，同时加大创新方面的投资，如自动化、机器学习、人工智能等，这将有助于重构未来所需人才队伍结构
行动措施 4.1.1	下一任总统应启动一个国家网络人才队伍培养项目，到 2020 年培养 100 000 名新的网络安全从业者（短期）
行动措施 4.1.2	下一任总统应启动一个国家网络安全新人培养项目，到 2020 年培养 50 000 名新的网络安全从业者（中期）
行动措施 4.1.3	为了更好地帮助学生将来成为联邦政府雇员，在为他们介绍和提供基于互联网的设备时，联邦政府支持的各级教育项目均应加入网络安全意识教育的内容（短期）
行动措施 4.1.4	联邦政府应开展强制培训项目，为管理者和行政人员培训网络安全风险管理相关内容，即使他们的主要职责不在网络安全领域，以便其在组织内建立网络安全文化（短期）
行动措施 4.1.5	联邦政府、SLTT 政府（州、地方、部落、领地）以及私营部门组织应建立一个交换项目，目的是提升中高级雇员的网络安全经验和能力（短期）
行动措施 4.1.6	美国人事管理局（OPM）应为联邦民事机构建立一个“总统网络安全研究员”项目，目的是到 2020 年培养 200 名网络安全专家（短期）
行动措施 4.1.7	NIST、国家科学基金会（NSF）、国家安全局（NSA）以及教育部应与私营组织、大学、专业社团合作，设立标准化的跨学科网络安全课程，以更好地融合、扩展现有活动和项目（中期）
行动措施 4.1.8	为了吸引更多学生参加网络安全学位项目，使其加入公共-私营部门的网络安全人才队伍，应制定鼓励政策，通过公共-私营合作等方式降低这些学生的债务，或补偿其教育支出（中期）

## 要求 5：使政府职能在数字时代得到有效和更安全的运转

建议 5.1	联邦政府应整合基础性的网络运营架构，提升对 IT 基础设施组件的共享利用能力
行动措施 5.1.1	联邦政府应启动一项工作，把所有民事机构的网络连接（也包括部分政府合同商）统一接入到一个网络中。此项工作和融合后的网络应由新成立的网络安全和基础设施保护机构（见行动措施 5.2.2）管理（中期）
建议 5.2	总统和国会应促进技术转化，加速联邦部门内的技术更新速度
行动措施 5.2.1	联邦政府应扩展近期建议的信息技术现代化基金会（ITMF），通过扩展预先确定的资金支持周期，资助对技术的投资。该基金会的投资应整合到 10 年滚动战略投资计划中，并成为预算规划过程的一部分，这与美国国防部（DoD）的操作方式类似（短期）
行动措施 5.2.2	美国总务管理局（GSA）应牵头将技术有效整合到政府的运行管理中，同时与国会合作，改革联邦采购要求，扩大对共享的标准服务平台的使用（中期）
建议 5.3	促使联邦机构从听命于网络安全要求的管理方式，转变到基于风险的管理方式
行动措施 5.3.1	美国管理和预算办公室（OMB）应对联邦机构提出要求，在任何网络安全相关报告、审查、政策修订和制定过程中使用“网络安全框架”（短期）

续表

行动措施 5.3.2	下届政府执政的前 100 天内,OMB 应与 NIST 和 DHS 合作,在“联邦信息安全现代化法”(FISMA)框架下,进一步明确相关机构和 OMB 的责任,并与“网络安全框架”协调一致(短期)
行动措施 5.3.3	OMB 应整合网络安全评价标准和机构绩效评估标准,并每两年修订一次,同时应把评估标准和相应的绩效融合到年度预算过程之中(短期)
建议 5.4	联邦政府应更好地将网络安全责任与总统行政办公室结构与职位进行匹配
行动措施 5.4.1	总统应任命并授权一位总统助理负责网络安全,并通过国家安全顾问向上汇报,该助理负责牵头制定国家网络安全政策和协调网络保护措施的实施(短期)
行动措施 5.4.2	联邦政府应明确 OMB 以及联邦首席信息官(CIO)、联邦首席信息安全官(CISO)、高级隐私顾问等在管理所有机构网络安全相关运行方面的角色(短期)
建议 5.5	各级政府应明确其在网络安全保护、防御、事件响应和恢复等方面的网络安全相关使命和责任
行动措施 5.5.1	总统应在其执政后的前 180 天内发布“国家网络安全战略”(短期)
行动措施 5.5.2	国会应把网络安全和基础设施保护功能整合到单一的联邦机构监管之下,同时要确保该机构具备完成其使命的相应能力与职责(短期)
行动措施 5.5.3	各州的州长应寻求适当的立法授权和资源,培训和装备国民警卫队,使其成为国家网络安全防御力量的组成部分(中短期)

#### 要求 6: 确保开放、公平、竞争和安全的全球数字经济发展

建议 6.1	联邦政府应鼓励并积极开展与国际组织的合作,制定和协调网络安全政策及最佳实践以及就网络安全法律和全球行为规范达成国际协定
行动措施 6.1.1	下届政府执政的前 180 天内,总统应任命一名网络安全大使,领导美国相关机构参与国际社会的网络安全战略、标准和最佳实践等相关活动(短期)
行动措施 6.1.2	联邦政府应提高在国际标准化领域的参与度,提高其他国家的广泛认可度,积极推动合理且协调一致的网络标准的使用(中期)
行动措施 6.1.3	美国国务院应继续与志同道合的国家开展合作,推动制定和平时期网络安全行为准则(短期)
行动措施 6.1.4	国会应为美国司法部提供充足的资源,为《法律互助条约》(MLAT)进程配备充足的人员,并使其适应新的情况,包括雇佣工程师、对高效率的技术进行投资等。国会也应修订美国法律,以便于在合理的司法调查中进行跨境电子证据访问。同时,还应为制定更广泛的框架和标准提供资源,以促进这类跨境访问(中期)
行动措施 6.1.5	NIST 和美国国务院应积极寻求国际合作伙伴,将“网络安全框架”中的风险管理方法推广到国际市场(短期)
行动措施 6.1.6	美国国务院、DHS 和其他机构,应继续根据不断增长的需求和发展趋势,为各国网络安全能力建设提供协助(短期)

---

## 三十三、强化美国网络安全和能力行政令 草案

美国总统特朗普签署前撤销<sup>①</sup>

2017 年 2 月 1 日

---

---

<sup>①</sup> 2017 年 2 月 1 日，特朗普在即将签署该行政令时，临时决定取消。美国社会普遍认为，该行政令的起草十分仓促，且没有明确联邦调查局（FBI）等部门的角色，取消签署实为必然。——译者注

利用美国宪法和法律赋予我作为总统的权力，现命令如下：

## 1. 政策

美国的政策是保护和加强国家网络基础设施的安全及能力。自由和安全地使用网络空间对于促进美国国家利益至关重要。互联网是重要的国家资源。网络空间必须成为有助于促进效率、创新、交流和经济繁荣的场所，不能出现破坏、欺诈、盗窃或隐私侵犯。美国致力于：确保国家在网络空间的长期实力；对这样一个与国际、国家和非国家行为体都相关的网络空间，保持美国能够决定性地塑造网络空间的能力；全面运用我们的能力来保卫美国在网络空间的利益；发现、阻断和击败恶意的网络行为体。

## 2. 发现

(a) 目前，美国的民事政府机构和关键基础设施极易受到国家和非国家行为体的攻击。犯罪分子、恐怖分子、国家和非国家行为体都投入到了持续行动之中，使美国经济遭受巨大损失，严重损害国家重大利益。这些行动可能会中断或破坏重要经济机构和关键基础设施的运行，并有可能带来潜在的物理影响，导致重大财产损失，甚至威胁生命。

(b) 技术创新的步伐，互联网应用的全球性、爆炸性增长，基础设施的网络及运行同关键经济机构之间日益增长的相互依赖性，以及不断演变的网络攻击和攻击者的性质，使网络领域正在经历持续、快速的变化。

(c) 这些变化使网络空间成为一个新的生存领域而兴起，就像陆地、海洋、天空以及太空一样重要，且其重要性还将在今后几年继续增强。

(d) 联邦政府有责任保护美国，防范网络攻击，以免威胁美国的国家利益，或者严重损害美国人民的安全或经济安全。这一责任包括保护私营及公共运营的关键网络和基础设施。同时，网络安全离不开活力、灵活性和创新性，这要求政府在履行责任时应与私营部门的实体密切合作。

(e) 目前，负责保护民事政府网络和关键基础设施的行政部、局（称为“机构”）还没有组织起来协同行动，它们任务不明、资源缺乏，也缺少成功履职所需的足够法律授权。

## 3. 定义

以本行政令中出现的先后为序：

(a) “关键基础设施”指对美国至关重要的物理或虚拟的系统和资产，这些系统和资产一旦失去运转能力或遭到破坏，会对国家安全、国家经济安全、国家公共健康和安全的的一个或多个方面造成破坏性影响。

(b) “国家安全系统”指的是任何由联邦政府或其合同商代表所运行的电信或信息系统，其功能、运行或使用：

- (i) 涉及情报活动；
- (ii) 涉及与国家安全相关的密码活动；
- (iii) 涉及军队的指挥和控制；
- (iv) 涉及武器或武器系统的装备；

(v) 对直接实现军队或情报使命至为关键(但不包括用于日常行政管理和商业应用的系统, 包括薪水支付、财务、后勤和人事管理应用)。

## 4. 政策协调

任何政策协调、指导方针、纠纷解决活动以及对本令中描述和指定的职能、项目所开展的定期进展评审, 均应通过 2017 年 1 月 21 日发布的第 1 号国家安全总统令中设立的跨部门流程(国家安全委员会和国土安全委员会的组织) 来实施, 或通过任何后继的流程来实施。

## 5. 网络脆弱性评估

(a) 范围和时限。

(i) 应立即启动对美国网络中最关键的脆弱性的评估。

(ii) 自本令发布之日起 60 天内, 应通过国防部部长向总统提交一份关于保护美国国家安全系统的初步建议。

(iii) 自本令发布之日起 60 天内, 应通过国土安全部部长向总统提交一份关于对最关键的民事联邦政府、公共-私营部门基础设施加强保护的初步建议, 美国国家安全系统除外。

(iv) 上述建议应包括具体步骤, 以确保责任机构能够被适当组织起来, 任务得以明确, 具备资源, 并且拥有完成任务所需的足够的法律权限。

(b) 评估参与者。国防部部长应与国土安全部部长、国家情报总监、总统国家安全事务助理、总统国土安全和反恐助理作为联合主席, 共同主持脆弱性评估。

(c) 脆弱性评估的运作。脆弱性评估联合主席应汇集联邦政府拥有的关于国家安全系统最紧急的脆弱性信息, 关于民事联邦政府的网络中最紧急的脆弱性信息以及最关键的私营部门基础设施的所有信息。所有机构应及时响应联合主席提出的任何信息请求, 提供自己掌握或控制的关于美国网络脆弱性的信息。国防部部长、国土安全部部长、总统国家安全事务助理、总统国土安全和反恐助理可以从任何适当来源处寻求与脆弱性评估相关的进一步信息。

## 6. 对网络对手的评估

(a) 范围和时限。

(i) 应立即启动对美国主要网络对手的评估。

(ii) 自本令发布之日起 60 天内, 应通过国家情报总监向总统提交关于美国主要网络对手的身份、能力和脆弱性的第一份报告。

(b) 评估参与者。国家情报总监应与国土安全部部长、国防部部长、总统国家安全事务助理、总统国土安全和反恐助理作为联合主席, 共同主持对手评估。

(c) 对手评估的运作。负责对手评估的联合主席应收集联邦政府拥有的与美国网络攻击者的身份、能力和脆弱性有关的所有信息。所有机构应及时响应联合主席提出的任何信息请求, 提供自己掌握或控制的关于美国网络对手的信息。联合主席可从任何适当来源处寻求与对手评

估有关的进一步信息。

## 7. 美国网络能力评估

(a) 范围和时限。

(i) 基于本行政令第 5 条和第 6 条的结果，应对国防部、国土安全部和国家安全局的相关网络能力进行评估，初步确定一组需要改进的能力集，以充分保护美国关键基础设施。

(ii) 能力评估的建议应包括具体步骤，以确保责任机构能够被适当组织起来，任务得以明确，具备资源，并且拥有完成任务所需的足够的法律权限。

(b) 评估参与者。国防部部长应与国土安全部部长和国家安全局局长作为联合主席，共同主持能力评估。

(c) 能力评估的运作。负责能力评估的联合主席应收集联邦政府拥有的关于国防部、国土安全部和国家安全局的相关网络能力的所有信息。所有机构应及时响应联合主席提出的任何信息请求，提供自己掌握或控制的关于美国网络能力的信息。国防部部长、国土安全部部长和国家安全局局长可以从任何适当的来源处寻求有关能力评估的进一步信息。

(d) 人才队伍发展评估。为了确保美国保持长期的网络能力优势，国防部部长和国土安全部部长还应收集和评估教育部从初级到中级高等教育中关于计算机科学、数学和网络安全教育的信息，以了解美国教育和培训未来人才队伍方面所做的全部努力。国防部部长应提出其认为合适的建议，以便最好地定位美国的教育制度，保持其未来的竞争优势。

## 8. 私营部门基础设施激励报告

(a) 范围和时限。

(i) 应立即启动编写一份报告，提出如何激励私营部门采用有效网络安全措施的选项。

(ii) 自本令发布之日起 100 天内，该报告所建议的选项应通过商务部部长向总统提交。

(b) 参与者。商务部部长将与财政部部长、国土安全部部长和总统经济事务助理作为联合主席，共同主持编写报告。商务部部长还可邀请证券交易委员会主席和联邦贸易委员会主席参与。

(c) 报告的运作。联合主席应审查和扩充现有的关于经济和其他激励措施的报告，以使国家关键基础设施的私人所有者和运营者最大程度地采取保护措施；对网络风险管理工具和服务进行投资；采取必要的关于流程和技术的最佳实践措施，以加强对实时网络威胁信息的共享和响应。所有机构应及时响应联合主席提出的任何信息请求，以确定能够促进对网络安全工具、服务和软件进行投资的有关经济政策和激励措施。财政部部长、商务部部长、国土安全部部长和总统经济事务助理可以从任何适当来源处寻求与报告有关的进一步资料。

## 9. 一般条款

(a) 本令的实施应符合可适用的法律，并受到拨款的制约。

(b) 本令的任何内容都不应解释为损害或以其他方式影响：

(i) 法律对行政部、局及其中任何负责人所赋予的权力；

(ii) 管理和预算办公室主任关于预算、行政或提出立法建议的职能。

(c) 根据本令采取的所有行动应符合保护情报和执法来源及方法的要求和授权。本令的任何内容都不应解释为取代现有法律授权下建立的保护特定活动及联络线的安全和完整性的措施，这些特定活动和联络线直接支持了情报和执法活动。

(d) 本令不拟也不会法律或正义角度制造任何会对美国及其各部局或其他实体、其官员或雇员以及任何其他个人造成触犯的权利或利益，不论是在实体方面还是流程方面。

---

## 三十四、 强化联邦网络和关键基础设施网络安全行政令草案

美国总统特朗普对已取消的行政令的修订<sup>①</sup>

2017 年 2 月 9 日

---

---

<sup>①</sup> 该草案是对 2017 年 2 月 1 日取消签署的行政令的修订，但未立即签署，而是在 5 月 11 日修改后正式发布。——译者注



利用美国宪法和法律赋予我作为总统的权力，现命令如下：

## 1. 联邦网络安全

(a) 政策。联邦政府行政部门代表美国人民，运营着政府自己的网络。这些网络及网络中的数据对所有的美国联邦政府职能而言都应当是安全可靠的。总统要求，各行政部、局的负责人（以下简称“机构负责人”）要对管理其机构的风险负责。此外，由于各机构负责人做出的风险管理决策可以影响到该行政部门的整体风险，故而美国政府的政策是将风险视作整个行政部门的事项来管理。

(b) 发现。

(i) 网络安全风险管理包括一系列用于标识和保护信息和 IT 资产的活动，防止其受到非授权访问及其他威胁，以保持对网络威胁的态势感知，检测不利于 IT 资产的异常现象和事件，减轻事件影响，响应事件并从中恢复。

(ii) 很久以来，行政部门的 IT 和信息系统陈旧，难以防护。

(iii) 有效的风险管理不仅仅限于保护当前在用的网络和数据，还要以合适的方式定期针对未来的维护、整改和现代化做出规划。

(iv) 已知但还没有修补的脆弱性是各行政部、局面临的最为严重的风险之一。这些脆弱性包括使用已超出供应商服务周期的操作系统或硬件，拒绝实施供应商的安全补丁，或者不遵循安全配置指南。

(v) 有效的风险管理要求各机构负责人带领一支由高级行政人员组成的综合性队伍，包括 IT、安全、预算、采购、法律、隐私和人力资源方面的专家。

(c) 风险管理。

(i) 总统要求各机构负责人要对落实风险管理措施负责，这些措施要与非授权访问、使用、泄露、中断、篡改、破坏信息或系统所造成的风险及危害程度相对应。总统还要求，各机构负责人要确保其信息安全管理过程与战略级、运行级和预算级的规划过程相一致，并符合《美国法典》第 44 编第 35 章第 II 小节的要求。

(ii) 即刻起，各机构负责人应有效地使用 NIST 发布的“增强关键基础设施网络安全框架”（以下简称“框架”）或后继文档，以管理本机构的网络风险。本令发布之日起 90 天内，每名机构负责人均应向管理和预算办公室主任及国土安全部部长提交一份风险管理报告，描述本机构对“框架”的实施情况。风险管理报告至少要记录各机构负责人采取的风险减缓措施和可接受的选项。如果选择了接受某未予处理的漏洞所带来的风险，则必须在报告中清晰记录此事。本段所提及的报告可以全部或部分标为涉密。

(iii) 在国土安全部部长的支持下，OMB 主任应根据《美国法典》第 44 编第 35 章第 II 小节的要求，评审每个机构的风险管理报告，以研判该报告中提出的风险管理选项是否在总体上可以有效并充分地管理好行政部门整体范围内的网络风险。

(iv) 经与国土安全部部长相协调，在商务部部长、总务管理局局长的支持下，OMB 主任应当在收到各机构风险管理报告的 60 天之内，通过总统国土安全和反恐助理向总统提交其研判结论以及一份计划，以：

(1) 针对所发现的行政部门的不足，提供足够的保护；

- (2) 建立定期评估和研判的流程;
- (3) 从研判结果出发, 指出行政部门风险管理所需的预算还有哪些没有得到满足;
- (4) 必要时澄清、调整、重新出台任何一个部门根据《美国法典》第 44 编第 35 章第 II 小节及本令所发布的所有的政策、标准、指南;
- (5) 使这些政策、标准、指南与“框架”相一致。
- (v) 美国的政策是, 建立一个更现代化的、更安全的和更有韧性的行政部门 IT 体系结构, 要即刻起实施以下活动:

(1) 各机构负责人要在其采购文档中说明如何在法律允许的最大范围内选择共享的 IT 服务, 包括电子邮件、云和网络安全服务。

(2) 总统跨政府和技术活动助理应当同商务部部长、国土安全部部长、OMB 主任、总务管理局局长共同协调制定一份提交给总统的报告, 内容是联邦政府的 IT 现代化。该报告应在本令发布之日起 150 天内完成, 且至少应包括以下内容:

① 使所有的机构迁移到一个或多个统一的网络体系结构上去的技术可行性和成本有效性、时间进度和里程碑, 以及实施这种迁移时遇到的任何的法律、政策、预算考虑。

② 使所有的机构迁移到共享的 IT 服务上去的技术可行性和成本有效性、时间进度和里程碑, 以及实施这种迁移时遇到的任何的法律、政策、预算考虑。

在讨论技术可行性时, 该报告还应考虑到向共享 IT 服务的迁移会给机构的信息安全带来何种影响, 包括提出有关建议, 确保符合《美国法典》第 44 编第 3553 条提出的政策和措施。所有的机构负责人均应提供本机构当前的 IT 体系结构和计划相关信息, 以便及时完成该报告。

(3) 对国家安全系统而言, 国防部部长和国家情报总监应当在可能的最大范围内实施本令。国防部部长和国家情报总监还应向总统国土安全和反恐助理提交一份报告, 描述其在本令发布后 150 天内落实本段要求的情况。本段所提及的报告可以全部或部分标为涉密。

## 2. 关键基础设施网络安全

(a) 政策。美国的政策是确保美国政府已准备好实施其授权和能力, 对国土安全部部长指定的关键基础设施实体的运营提供保护。

(b) 对关键基础设施的支持。经与国防部部长、司法部部长、FBI 主任、国家情报总监以及关键基础设施对口机构 (2013 年 2 月发布的 PDD21 中定义) 的负责人以及其他机构负责人 (由国土安全部部长指定) 相协调, 国土安全部部长应:

(i) 明确各机构为了支持关键基础设施所有者和运营者的网络安全工作, 需要具备什么样的授权和能力。这些关键基础设施是 2013 年 2 月 12 日第 13636 号总统令“增强关键基础设施网络安全”第 9 节规定的“面临最大攻击风险”的基础设施, 其可能导致灾难性的地区或国家级影响, 涉及公共健康和安全、经济安全或国家安全。

(ii) 与“增强关键基础设施网络安全”第 9 节所提实体合作, 并在必要时听取其意见, 评估第 (i) 节明确的授权和能力是否以及如何能够支持其风险管理工作, 并找出任何可能

的障碍。

(iii) 自本令签署之日起 180 天内，应通过总统国务安全和反恐助理，向总统提交一份报告，必要时可以包含涉密的附件，内容有：

(1) 根据本段要求所确定的授权和能力。

(2) 根据本段要求，与关键基础设施所有者和运营者的接触情况以及所需的决定。

(3) 为了更好地支持“增强关键基础设施网络安全”第 9 节规定的实体的网络安全工作，有哪些结论和建议。

(c) 支持市场透明性。经与商务部部长相协调，通过总统国土安全和反恐助理，国土安全部部长应当向总统提交一份报告，检查现有的联邦政策和措施是否足以促进关键基础设施实体所采用的网络安全风险管理措施的市场透明性，而且要侧重于公共贸易领域的关键基础设施实体。

(d) 核心通信基础设施。经与国土安全部部长相协调，商务部部长应牵头启动一项公开和透明的进程，为核心通信基础设施的所有者、运营者和其他利益相关方确定行动方案，并推动其采取行动，以增强这类基础设施的韧性，极大地减轻自动化和分布式攻击（如僵尸网络）带来的威胁。在落实本段的要求时，商务部部长和国土安全部部长应咨询国防部部长、司法部部长、FBI 主任、关键基础设施对口机构负责人、联邦通信委员会主席、联邦贸易委员会主席、其他感兴趣的机构负责人、核心通信基础设施的所有者和运营者以及其他相关的利益相关方。本令发布之日起 240 天内，商务部部长和国土安全部部长应就此项工作的进展公开发布报告。本令发布之日起 1 年内，商务部部长和国土安全部部长应向总统提交最终报告。

(e) 对断电响应能力的评估。虽然本令的实施是为了提高关键基础设施的安全性，但国土安全部部长还应与能源部部长相协调，并咨询州、地方、部落和领地政府以及其他合适的利益相关方，以评估：

(i) 美国电力部门可能遭到的重大网络事件的影响范围和持续期；

(ii) 美国对管理此类事件后果是否做好了准备；

(iii) 为了减轻这类事件的影响，还缺少哪些资产和能力。

本令发布之日起 90 天内，评估结果应通过总统国土安全和反恐助理向总统提交，必要时可包含涉密的附录。

(f) 国防部作战能力和工业基地。本令发布之日起 90 天内，经与国家情报总监相协调，国防部部长和国土安全部部长、FBI 主任应通过总统国家安全事务助理、总统国土安全和反恐助理向总统提交报告，说明国防工业基地面临的网络安全风险，包括供应链风险以及美国军事平台、系统、网络和功能面临的网络安全风险，并就如何减缓这些风险提出建议。

### 3. 国家网络安全

(a) 政策。美国的政策是促进一个开放、互操作、可靠和安全的互联网，促进效率、创新、交流和经济繁荣，尊重隐私，防范破坏、欺诈和盗窃。

(b) 威慑和保护。本令发布之日起 90 天内，经与国家情报总监相协商，国务卿、财政部部长、国防部部长、司法部部长、商务部部长、国土安全部部长和美国贸易代表应联合向总统提交报告，说明国家为威慑敌人、更好地保护美国人民可以采取的战略选项，防止敌人利用网络化技术击败或破坏本令提出的政策。

(c) 互联网自由和治理。互联网是支撑美国力量、创新和价值的源泉。本令发布之日起 180 天内，经与司法部部长相协商，国务卿、财政部部长、国防部部长、商务部部长和国土安全部部长应向总统提交报告，说明如何采取持续行动来支持多利益相关方进程，以确保互联网面向未来仍保留其重要、可靠和安全的特性。

#### 4. 一般条款

(a) 本令的任何内容都不应解释为损害或以其他方式影响：

(i) 法律对行政部、局及其中任何负责人所赋予的权力；

(ii) 管理和预算办公室主任关于预算、行政或提出立法建议的职能。

(b) 根据本令采取的所有行动应符合保护情报和执法来源及方法的要求和授权。本令的任何内容都不应解释为取代现有法律授权下建立的保护特定活动及联络线的安全和完整性的措施，这些特定活动和联络线直接支持了情报和执法活动。

(c) 本令不拟也不会法律或正义角度制造任何会对美国及其各部局或其他实体、其官员或雇员以及任何其他个人造成触犯的权利或利益，不论是在实体方面还是在流程方面。

---

## 三十五、强化联邦网络和关键基础设施网络安全行政令

白宫

2017年5月11日

---

利用美国宪法和法律赋予我作为总统的权力，为保护美国的创新力和价值观，现命令如下：

## 1. 联邦网络安全

(a) 政策。联邦政府行政部门代表美国人民运营着政府自己的网络。这些网络及网络中的数据对所有的美国联邦政府职能而言都应当是安全可靠的。总统要求，各行政部、局的负责人（以下简称“机构负责人”）要对管理其机构的风险负责。此外，由于各机构负责人做出的风险管理决策可以影响到该行政部门的整体风险，故而美国政府的政策是将风险视作整个行政部门的事项来管理。

(b) 发现。

(i) 网络安全风险管理包括一系列用于保护 IT 和数据的活动，防止其受到非授权访问及其他网络威胁，以保持对网络威胁的态势感知，检测不利于 IT 和数据的异常现象和事件，减轻事件影响，响应事件并从中恢复。信息共享促进和支持所有这些活动。

(ii) 很久以来，行政部门的 IT 陈旧，难以防护。

(iii) 有效的风险管理不仅仅限于保护当前在用的网络和数据，还要以合适的方式定期针对未来的维护、整改和现代化做出规划。

(iv) 已知但还没有修补的脆弱性是各行政部、局面临的最为严重的风险之一。这些脆弱性包括使用已超出供应商服务周期的操作系统或硬件，拒绝实施供应商的安全补丁，或者不遵循安全配置指南。

(v) 有效的风险管理要求各机构负责人带领一支由高级行政人员组成的综合性队伍，包括 IT、安全、预算、采购、法律、隐私和人力资源方面的专家。

(c) 风险管理。

(i) 总统要求各机构负责人要对落实风险管理措施负责，这些措施要与非授权访问、使用、泄露、中断、篡改、破坏 IT 和数据所造成的风险及危害程度相对应。总统还要求，各机构负责人要确保其信息安全管理过程与战略级、运行级和预算级的规划过程相一致，并符合《美国法典》第 44 编第 35 章第 II 小节的要求。

(ii) 即刻起，各机构负责人应有效地使用 NIST 发布的“增强关键基础设施网络安全框架”（以下简称“框架”）或任何后继文档，以管理本机构的网络风险。本令发布之日起 90 天内，每名机构负责人均应向国土安全部部长及管理和预算办公室主任提交一份风险管理报告。该风险管理报告应：

(1) 记录各机构负责人自本令发布之日采取的风险减缓措施和可接受的选项，包括：

(A) 影响这些选项的战略级、运行级和预算级考虑；

(B) 如果选择了接受某未予处理的漏洞，所带来的风险。

(2) 描述本机构对“框架”的实行动计划。

(iii) 国土安全部部长和 OMB 主任应根据《美国法典》第 44 编第 35 章第 II 小节的要求，共同评审每个机构的风险管理报告，以研判该报告中提出的风险减缓措施和可接受的选项是否在总体上可以有效并充分地管理好行政部门整体范围内的网络安全风险（研判结论）。

(iv) 经与国土安全部部长相协调，在商务部部长、总务管理局局长的支持下，OMB 主任应当在收到本节第 (c) 条第 (ii) 款所述各机构风险管理报告的 60 天之内，通过总统国土安全和反恐助理向总统提交以下内容：

- (1) 研判结论；
- (2) 一份计划，以：
  - (A) 针对所发现的行政部门的不足，提供足够的保护；
  - (B) 立即处理行政部门风险管理所需的、没有得到满足的预算；
  - (C) 建立定期评估、研判和处置流程，适当情况下重新研判并解决未来行政部门风险管理必要的、却常常没有得到满足的预算需求；
  - (D) 必要时且在法律允许的范围内，澄清、调整、重新出台任何部门根据《美国法典》第 44 编第 35 章第 II 小节所发布的所有的政策、标准、指南以及根据本令，出台政策、标准、指南；
  - (E) 使这些政策、标准、指南与“框架”相一致。

(v) 本节第 (c) 条第 (ii) 款所述各机构风险管理报告以及第 (c) 条第 (iii) 款和第 (iv) 款所述研判结论和计划可以根据情况全部或部分标密。

(v) 行政部门的政策是，建立一个更现代化的、更安全的和更有韧性的行政部门 IT 体系结构，要即刻起实施以下活动：

(1) 各机构负责人要在其采购文档中说明如何在法律允许的最大范围内选择共享的 IT 服务，包括电子邮件、云和网络安全服务。

(2) 美国技术委员会主任应当同国土安全部部长、OMB 主任、总务管理局局长共同协调制定一份提交给总统的报告，必要时还应咨询商务部部长，报告内容是联邦政府的 IT 现代化。该报告应：

- (A) 在本令发布之日起 90 天内完成；
- (B) 描述使所有或部分机构迁移到以下系统时相关的法律、政策、预算考虑，以及技术可行性和成本有效性，包括时间进度和里程碑，迁移到的系统可以是：
  - ① 一个或多个统一的网络体系；
  - ② 共享的 IT 服务，包括电子邮件、云和网络安全服务。

(3) 本节第 (c) 条第 (vi) 款第 (2) 项所述报告应对所有或部分机构向共享 IT 服务的迁移会给机构的网络安全带来何种影响进行评估，包括提出有关建议，确保符合《国土安全法》(6 U.S.C. 148) 第 227 节以及《美国法典》第 44 编第 3553 条提出的政策和措施。所有的机构负责人均应提供本机构当前的 IT 体系结构和计划相关信息，以便及时完成该报告。

(4) 对国家安全系统（定义参见《美国法典》第 44 编第 3552 条 (b) (6) 项）而言，国防部部长和国家情报总监，而非国土安全部部长和 OMB 主任，应当在可能的最大范围内实施本令。国防部部长和国家情报总监还应向总统国家安全事务助理以及总统国土安全和反恐助理提交一份报告，描述其在本令发布后 150 天内落实本节第 (c) 条要求的情况。本段所提及的报告应包括对任何不符合第 (c) 条要求的情况的解释，报告可以全部或部分标为涉密。

## 2. 关键基础设施网络安全

(a) 政策。行政部门的政策是适当时，运用其授权和能力对国家关键基础设施所有者和运营者的网络安全风险管理活动提供支持，“关键基础设施”的定义参见《美国法典》第 42 编第 5195 条 c (e) 款有关“关键基础设施实体”的定义。

(b) 对风险最大的关键基础设施的支持。经与国防部部长、司法部部长、国家情报总监、FBI 主任以及关键基础设施对口机构（2013 年 2 月 12 日发布的 PDD21 “关键基础设施的安全和韧性”中定义）的负责人以及其他机构负责人（由国土安全部部长指定）相协调，国土安全部部长应：

(i) 明确各机构为了支持关键基础设施实体的网络安全工作，需要具备什么样的授权和能力。这些关键基础设施是 2013 年 2 月 12 日第 13636 号总统令“增强关键基础设施网络安全”第 9 节规定的“面临最大攻击风险”的基础设施，其可能导致灾难性的地区或国家级影响，涉及公共健康和安全、经济安全或国家安全。

(ii) 与“增强关键基础设施网络安全”第 9 节所提实体合作，并在必要时听取其意见，评估本节第 (b) 条第 (i) 款明确的授权和能力是否以及如何能够支持网络安全风险管理工作的，并找出任何可能的障碍。

(iii) 自本令签署之日起 180 天内，应通过总统国土安全和反恐助理，向总统提交一份报告，必要时可以全文或部分涉密，内容有：

(1) 根据本节第 (b) 条第 (i) 款要求所确定的授权和能力。

(2) 根据本节第 (b) 条第 (ii) 款要求进行的接触情况以及所需的决定。

(3) 为了更好地支持“增强关键基础设施网络安全”第 9 节规定的实体的网络安全工作，有哪些结论和建议。

(iv) 此后每年更新报告并向总统提交。

(c) 支持市场透明性。自本令签署之日起 90 天内，经与商务部部长相协调，通过总统国土安全和反恐助理，国土安全部部长应当向总统提交一份报告，检查现有的联邦政策和措施是否足以促进关键基础设施实体所采用的网络安全风险管理措施的市场透明性，而且要侧重于公共贸易领域的关键基础设施实体。

(d) 抵御僵尸以及其他自动化和分布式威胁的韧性。商务部部长和国土安全部部长应共同启动一项公开和透明的进程，确定并利益相关方的行动方案，并推动其采取行动，以增强互联网和通信生态系统的韧性，鼓励合作，从而极大地减轻自动化和分布式攻击（如僵尸网络）带来的威胁。在落实本段的要求时，商务部部长和国土安全部部长应咨询国防部部长、司法部部长、FBI 主任、关键基础设施对口机构负责人、联邦通信委员会主席、联邦贸易委员会主席、其他感兴趣的机构负责人以及其他有关利益相关方。本令发布之日起 240 天内，商务部部长和国土安全部部长应就此项工作的进展公开发布报告。本令发布之日起 1 年内，商务部部长和国土安全部部长应向总统提交最终报告。

(e) 对断电响应能力的评估。经咨询国家情报总监，州、地方、部落、领地政府以及合适的其他相关方，能源部部长和国土安全部部长应共同评估：

(i) 美国电力部门可能遭到的重大网络事件的影响范围和持续期，“重大网络事件”的定义参见 2016 年 7 月 26 日发布的 PDD 41 “美国网络事件协调”；



(ii) 美国对管理此类事件后果是否做好了准备；

(iii) 为了减轻这类事件的影响，还缺少哪些资产和能力。

本令发布之日起 90 天内，评估结果应通过总统国土安全和反恐助理向总统提交，必要时可全文或部分涉密。

(f) 国防部作战能力和工业基地。本令发布之日起 90 天内，经与国家情报总监相协调，国防部部长和国土安全部部长、FBI 主任应通过总统国家安全事务助理、总统国土安全和反恐助理向总统提交报告，说明国防工业基地面临的网络安全风险，包括供应链风险以及美国军事平台、系统、网络和功能面临的网络安全风险，并就如何减缓这些风险提出建议。必要时，报告可以全文或部分涉密。

### 3. 国家网络安全

(a) 政策。为确保互联网对后世来说仍有价值，行政部门的政策是促进一个开放、互操作、可靠和安全的互联网，促进效率、创新、交流和经济繁荣，尊重隐私，防范破坏、欺诈和盗窃。此外，作为实现网络空间目标的基础，美国力求提高网络安全和相关领域技术熟练的人员的数量并加以维持。

(b) 威慑和保护。本令发布之日起 90 天内，经与国家情报总监相协商，国务卿、财政部部长、国防部部长、司法部部长、商务部部长、国土安全部部长和美国贸易代表应通过总统国家安全事务助理、总统国土安全和反恐助理联合向总统提交报告，说明国家为威慑敌人、更好地保护美国人民免受网络威胁可以采取的国家战略选项。

(c) 国际合作。互联网是支撑美国国力、创新和价值的源泉。美国是一个高度互联的国家，尤其依赖于全球范围内安全可靠的互联网，因此必须与盟国和其他合作伙伴共同努力以维护本节提出的政策。本令发布之日起 45 天内，经与司法部部长和 FBI 主任相协商，国务卿、财政部部长、国防部部长、商务部部长和国土安全部部长应向总统提交报告，说明国际上网络安全的优先事项，包括有关调查、溯源、网络威胁信息共享、响应、能力建设和合作的事项。该报告提交之日起 90 天内，经与本段列举的及其他有关机构的负责人相协商，国务卿应通过总统国土安全和反恐助理向总统提交报告，给出参与网络安全国际合作的战略。

(d) 人员建设。为了确保美国长期具备网络安全优势：

(i) 经咨询国防部部长、劳工部部长、教育部部长、人事管理办公室主任以及由商务部部长和国土安全部部长共同指定的其他机构，商务部部长和国土安全部部长应：

(1) 共同评估为教育和培养美国未来网络安全人员而做出的努力的范围与充分性，包括从小学到高等教育的网络安全相关教育课程、培训和实习计划。

(2) 本令发布之日起 120 天内，通过总统国土安全和反恐助理联合向总统提交报告，说明为推动提高国家公共和私有部门网络安全人员的数量并加以维持，有哪些结论和建议。

(ii) 经咨询由其指定的其他机构负责人，国家情报总监应：

(1) 评估潜在的外国网络同行的人员建设活动，以便发现可能影响美国网络安全长期竞争力的外国人员建设实践。

(2) 本令发布之日起 60 天内，通过总统国土安全和反恐助理联合向总统提交报

告，说明根据本节第（d）（ii）（1）项得出的评估结论。

（iii）经咨询商务部部长，国土安全部部长和国家情报总监应：

（1）评估美国为保持或提升其国家安全相关网络能力优势而做出的努力的范围和充分性。

（2）本令发布之日起 150 天内，通过总统国土安全和反恐助理联合向总统提交报告，说明根据本节第（d）（iii）（1）项的评估，有哪些结论和建议。

（iv）本段所述报告可以全文或部分涉密。

## 4. 定义

在本令中：

（a）术语“有关利益相关方”指根据本令第 2 节第（d）条，选择参与由商务部部长和国土安全部部长共同建立的一项公开和透明的进程的任何非行政机构个人或实体。

（b）术语“信息技术”（IT）的定义参见《美国法典》第 40 编 11101（6）条有关定义，并且还包括机构用于监控物理设备和流程的硬件或软件系统。

（c）术语“IT 架构”指一个机构中 IT 的整合与实施。

（d）术语“网络架构”指 IT 架构中使两个或多个 IT 资产能够进行通信的元素，或者使这种通信变得更加便捷的元素。

## 5. 一般条款

（a）本令的任何内容都不应解释为损害或以其他方式影响：

（i）法律对行政部、局及其中任何负责人所赋予的权力；

（ii）管理和预算办公室主任关于预算、行政或提出立法建议的职能。

（b）本令的实施应符合有关法律规定并受制于可用拨款的多少。

（c）根据本令采取的所有行动应符合保护情报和执法来源及方法的要求和授权。本令的任何内容都不应解释为取代现有法律授权下建立的保护特定活动及联络线的安全和完整性的措施，这些特定活动和联络线直接支持了情报和执法活动。

（d）本令不拟，也不会法律或正义角度制造任何会对美国及其各部局或其他实体、其官员或雇员以及任何其他个人造成触犯的权利或利益，不论是在实体方面还是在流程方面。

——特朗普

2017 年 5 月 11 日

---

## 三十六、保护网络资产：应对关键基础设施面临的紧迫网络威胁（草稿）

国家基础设施总统咨询委员会（NIAC）

2017 年 8 月

---

## 1. 执行摘要——要点导读

通过分析数百项研究以及对 38 位网络和行业专家的访谈，我们认识到应立即采取行动保护美国关键基础设施免受具有侵略性和针对性的网络攻击。网络空间是唯一由私营企业站在基础设施国家攻击防御前线的竞技场。当网络攻击产生与物理攻击相同的破坏后果时，需要国家层面的领导以及在资源、职能等方面的密切协作。

### 评估

国家安全委员会（NSC）委托国家基础设施总统咨询委员会（NIAC）评估，如何充分发挥联邦机构和职能的作用来保护高风险资产的网络安全。为了完成这项工作，我们对一个涵盖 140 多个联邦机构和职能的综合数据集进行了评估，该数据集展现了联邦资源的深度和复杂性。

我们认为美国政府和私营部门拥有强大的网络能力和广泛的资源，合理组织和集中运用这些能力和资源，能够保护私营关键系统免受侵略性网络攻击。当前，我们还有不足之处。

### 建议

NIAC 提出的挑战被广泛认可并多次出现在相关研究中。在“9·11”规模的网络攻击出现前，我们有一个短暂的窗口期来组织采取果断有效的行动。我们呼吁政府利用这一窗口期采取以下具有决定性的行动。

（1）为最关键的网路建立**独立、安全的专用通信网**，包括用于关键控制系统流量的“暗光纤”网络和用于备用紧急通信的预留频谱。

相关机构：能源部（DOE）、国土安全部（DHS）、国家情报总监办公室（ODNI）、国家安全委员会（NSC）和战略基础设施协调委员会（SICC）（电力、金融服务和通信行业）。

（2）电力和金融服务部门牵头，**推动由私营部门主导的机器到机器信息共享技术试点**，以测试公共-私营部门以及企业间网络威胁信息共享是否达到网络速度。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

（3）明确技术领先的**扫描工具和评估实践**，并与关键基础设施所有者和运营者合作，以自愿形式对其系统进行扫描和评估。

相关机构：NSC、DHS 和国会。

（4）通过资助公共和私营部门专家交流项目，**增强当前网络人才队伍**的专业能力。

相关机构：NSC、DHS 和国会。

（5）建立一套**具有时限的、以成果为导向的市场激励措施**，鼓励关键基础设施所有者和运营者升级其网络基础设施，投资发展最先进的技术，以符合行业标准或最佳实践要求。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

（6）简化并显著加快对国家最关键的网路资产所有者的**安全许可审批**，提升敏感区域信息设施（SCIF）配置、可用性和易用性，以确保获得安全许可的关键基础设施所有者和运营者可以在主要威胁或事件发生 1 小时内访问安全设施。

相关机构：DHS、ODNI、NSC、联邦调查局（FBI）、人事管理局（OPM）以及所有发起或支持审批的机构。

（7）制定清晰的**网络威胁信息快速解密方案**，主动与处于国家网络攻击防御前线的关键基

基础设施所有者和运营者分享网络威胁信息。

相关机构：NSC、DHS、ODNI、FBI 和情报共同体（IC）。

（8）作为试点，成立由政府专家和电力、金融和通信行业专家组成的行动小组，小组由拥有决策权的高级管理人员领导，配置资源，面对不断升级的网络威胁，从国家最高网络需求出发采取果断、快速、灵活的行动。

相关机构：DOE、DHS、ODNI、NSC、SICC、国防部（DOD）、财政部和司法部（DOJ）。

（9）计划于 2017 年 11 月举行国家级 GRIDEX IV 网络演习，测试联邦机构及职能在网络事件中的执行情况，并向具体机构提出针对性建议，以协调和明确联邦政府尚未明确的响应行动。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

（10）制定最佳的网络安全治理方案，整合不同联邦机构的资源和专业能力，以指导和协调国家网络防御。

相关机构：DHS、ODNI、NSC、DOJ 和 DoD。

（11）由国家安全顾问评估本报告提出的建议，并在 6 个月内召开政府高级官员会议，以扫清实施障碍，并明确下一步工作安排。

相关人员：国家安全顾问。

行动刻不容缓。我们国家需要从过去简单研究网络安全挑战转为采取有意义的战略举措，以增强国家网络安全，阻止重大网络攻击的发生。

为了显著降低网络风险，我们国家需要明确方向和领导机制。NIAC 已做好准备，继续在这一领域为总统提供支持。

## 2. 介绍

当前，高级攻击者发动的网络攻击越发危险、针对性强，这些网络攻击可对提供电力和金融等重要服务的关键基础设施造成破坏，甚至导致运行中断。通过渗透控制物理过程的数字系统，攻击者不需要进行物理攻击就能破坏专用设备并中断重要服务，进而对物理设施造成破坏。在针对基础设施的国家攻击中，私营企业站在防御前线，这与我们面临的其他国家安全挑战不同。联邦政府和私营部门在保护信息系统方面存在共同利益，需要相互支持。

NIAC 认为美国政府和私营部门拥有巨大的网络能力和资源，通过合理组织和集中运用这些能力和资源，能够保护私营关键系统免受具有侵略性的网络攻击。当前我们面临的问题是，网络安全职能和监管分散、角色和责任划分不清，以及工作组织尚未跟上威胁的变化。

幸运的是，我们尚处于“9·11”规模网络攻击发生前的阶段，有短暂的窗口期来有效协调相关资源。我们呼吁政府利用这一窗口期勇于采取决定性行动，这些行动需要联邦政府运用其行政权力和职能来与私营部门开展合作。

### 任务

为落实 2017 年 5 月发布的第 13800 号总统行政令“加强联邦网络 and 关键基础设施的网络安全”的要求，国家安全委员会（NSC）委托 NIAC 评估如何充分利用现有联邦机构及职能来帮助和更好地保护最容易遭受网络攻击的关键基础设施资产的网络安全，这些关键基础设施资产一旦遭到破坏，将在公共健康或公共安全、经济安全或国家安全等方面对国家或地区产生灾

难性影响。为完成此项工作，NIAC 成立了一个 9 人工作组。

### 评估

工作组得到了一个有关 140 多个不同联邦机构及职能的综合数据集，包括多个项目和独立行动。该数据集展现了巨大的联邦现有职能，也凸显了联邦结构和机制的复杂性。我们首先分析了当前高风险行业的最大需求，然后研究如何利用现有联邦机构和职能来解决这些问题。

研究发现，许多杰出的联邦职能在保障网络防御和韧性方面可发挥至关重要的作用。然而受以下限制，这些职能未能有效发挥：

- 私营部门对相关联邦职能和利用这些职能的激励措施了解有限。
- 对相关联邦职能的获取受到诸多法律和行政限制。
- 政府能力分散在大量机构、部门及其分支机构中，没有形成有效的职能检索机制。
- 基础威胁信息的分类可能会延迟和阻碍协调响应。

## 3. 建议和依据

通过分析数百项研究和对 38 位网络和行业专家的访谈，我们认识到当前面临巨大挑战，需要尽快采取行动。**NIAC 在本报告中提出的挑战被广泛认可**并多次出现在 NIAC 相关研究中，国家网络安全促进委员会（CENC）最近对其进行了更详细的介绍。

NIAC 的特有价值在于，**从高级私营部门所有者和运营者的角度出发，对政府和私营部门如何更好地协作来保护最关键的基础设施资产提出见解**。我们知道，这些建议提出的协调水平并不易达到，因此建议与最关键的部门共同建立创新性解决方案试点。这些部门面临的网络安全紧迫性高，而且高层领导已经参与到试点中。

我们详细研究了当前的网络安全挑战，并准备采取行动。以下提出的 11 条建议反映了对下一步行动的强烈共识。（附录 C 和 D 提供了更多背景信息，附录 E 列出了参考资料。）

### 建议 1

为最关键的网路建立**独立、安全的专用通信网**，包括用于关键控制系统流量的“暗光纤”网络和用于备用紧急通信的预留频谱。

（1）启动试点项目，识别已有但未使用或未充分使用的光纤网络（即“暗光纤”），为关键基础设施部门建立专用通信网络。通过试点论证是否能够不通过公共网络来操作关键控制系统，从而使网络攻击者难以访问。

（2）构建安全备用通信系统，确保在发生跨部门重大网络攻击时保持实时通信。该通信系统预留一部分电磁频谱，将实时通信与互联网或基于网络的通信分离。例如，在电力企业遭受网络攻击后，利用备用通信系统支持电力企业与现场工作人员联络，手动恢复电力供应。

相关机构：DOE、DHS、ODNI、NSC 和 SICC（电力、金融服务和通信）。

#### （3）依据

①对数字和物理基础设施系统网络攻击的规模、范围和频率正迅速增加。随着更多有经验和有组织的攻击者开始策划有针对性的攻击，以破坏或扰乱重要服务和关键物理系统，网络威胁形势日益严峻。

- 目前的网络威胁具有双重性：一是针对信息技术（IT）的攻击，包括支撑金融服务等关键部门业务功能的软件和网络；二是针对运营技术（OT）的攻击，包括用于操作物理过程的控制系统，如电网中的电力流。

②与业务 IT 系统和互联网连接的工业控制系统造成了关键基础设施中的系统性网络风险。联网的 OT 系统提高了关键流程控制的自动化程度和效率（如电力、水、燃料以及化学制品的生成、处理和交付等），但同时也引入了新的网络风险。

③一些电力企业正在将其运营的系统向专用和封闭的网络迁移，减少从通信服务商处租用的共享线路。使用专用网络可以显著减少接入点数量，从而减少企业运营人员所需防护的风险点。

④当发生重大网络攻击破坏主通信网（互联网、电子邮件、电话和手机通信）时，备用网络将出现拥堵和不稳定。政府可以为关键基础设施通信提供专用频谱，以加快响应和恢复速度。

## 建议 2

电力和金融服务部门牵头，**推动由私营部门主导的机器到机器信息共享技术试点**，以测试公共-私营部门以及企业间网络威胁信息共享是否达到网络速度。

（1）利用试点确认和评估最先进的技术和软件平台，解决互操作性和隐私问题，以及当前阻碍或限制公司之间、政府与企业之间信息共享的法律和责任问题。

（2）充分利用现有的在公共-私营部门之间快速共享网络威胁和攻击迹象信息的平台，加强建设和协调，包括：

①能源部网络安全风险信息共享项目（CRISP），该项目由电力信息共享和分析中心（E-ISAC）运营，通过网络流量分类分析方法来识别攻击。

②金融服务信息共享和分析中心（FS-ISAC）机器到机器信息共享计划，目前已被部分能源机构使用。

③国土安全部自动指标共享（AIS）平台，该平台通过多渠道发布攻击迹象。

（3）信息共享和分析中心（ISAC）可利用从试点中学到的经验形成平台、方案和最佳实践，将试点扩大到其他关键部门，并适时开展机器到机器信息共享研发。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

（4）依据。

①公共-私营部门仍然无法及时准确地传输网络威胁相关信息。威胁信息和缓解方法必须按照网络速度传输。研发机器到机器信息共享和自动缓解方法具有重要的应用前景。

②机器到机器信息共享技术和程序尚未成熟，必须克服重大的法律、责任、技术、信任和成本挑战。试点将为协调以下关键问题提供实践依据：

- 与联邦政府安全地共享实时系统数据需要在信息保护、共享和使用方面获得充分信任。数据泄露将造成重大商业风险，责任问题尚未经过法律检验。
- 机器到机器信息共享需要统一的通用技术、数据格式、方案和策略。
- 自动执行缓解程序可能会对运行控制环境产生未知影响。
- 对攻击迹象进行自动共享可能导致运行人员埋没在海量数据中，难以解析和优先排序。

③最有效且附加值高的平台将支持公共-私营部门之间以及企业与企业之间的信息交换。

- 私营部门拥有更多的原始实时网络数据，并且企业与企业之间的信息共享往往更快。

- 政府通过对不同企业的信息进行关联分析,更有助于发现潜在威胁、增加情报理解力、了解威胁意图和发出警报。当前,对威胁进行验证分析并经允许进行共享,所需的时间明显太长了。
- 企业可以更好地引导开发满足其需求的解决方案。

④各行业间的组织形式、行业信任和成本、成员维系和发展模式、资源水平等各有不同,故 ISAC 信息共享的有效性差异明显。但 ISAC 仍是从情报共同体获得威胁信息和企业之间信息交换的重要渠道。工作高效的 ISAC 应作为其他部门的典范,以促进信息共享。

### 建议 3

明确技术领先的**扫描工具和评估实践**,并与关键基础设施所有者和运营者合作,以自愿形式对其系统进行扫描和评估。

(1) 建立一个自愿的、费用共担的扫描和评估项目,提供现场扫描工具和专业知识以帮助组织:①使用技术领先的工具测试组织系统内是否有恶意软件;②清理系统;③明确政府和行业工具提供商和服务提供商,便于升级和维护系统安全。

(2) 建立卓越中心,展示行业技术领先的工具,并为企业(特别是中小型企业)提供试验台环境和新软件评估服务;认可、使用和扩大现有教育机构的网络安全项目。

相关机构: NSC、DHS 和国会。

(3) 依据

①通常情况下,管理者没有完全了解他们所面临风险的大小或复杂性,以及威胁可能对其系统造成破坏的程度。

- 网络安全研究人员的报告指出,全世界超过 30%的计算机可能存在恶意代码或恶意软件,但很少有公司了解其面临的潜在威胁。
- 实际上,联邦政府拥有大量网络安全工具,可为企业提供扫描、检测、减轻和抵御网络威胁的服务。但是,许多企业缺乏利用联邦工具的意识,尽管有这些有效的工具和实践,也没有进行基本的网络安全检测。

②关键系统的所有者可能是财富 100 强企业也可能是一家小型公司,具有不同的风险、资源和网络安全需求,因此需要定制化的解决方案。

- 对于网络安全成熟度较低的实体或针对大范围网络攻击,政府的工具或能力通常可以发挥重大作用。

③对关键基础设施运营者来说,供应链风险仍是一项挑战。目前,运营者仍缺乏可靠的方法来验证数字元件的来源,无法对数字元件的设计、制造、集成和使用进行监督。

- 目前,我们仍无法检测嵌入式威胁或验证关键 OT 系统设备的安全性。能源部、国家实验室和国土安全部可与电力行业和元件制造商合作,研发面向行业的解决方案来验证 OT 系统设备的供应链安全。

### 建议 4

通过资助公共-私营部门专家交流项目,增强**当前网络人才队伍**的专业能力。

(1) 实施公共和私营部门员工交流计划,帮助联邦雇员更好地了解关键基础设施日常运营和网络系统的作用。该项目可推动联邦政府更好地研制相关方案和工具并识别资源,帮助私营部门应对网络风险,扫清私营部门使用联邦工具和服务的障碍。对于私营部门员工来说,该计



划有助于更好地了解联邦政府的项目、工具和资源。

(2) 联邦和国会将扩大网络人才队伍计划列为工作重点，根据第 13800 号总统行政令要求的审核结果，建立可持续机制，以解决合格网络人才缺乏的问题。

①国会也应考虑扩大奖学金计划，重点加强下一代网络人才队伍建设。

②为参与网络安全计划的大学生提供资助，帮助其快速成长为合格的网络人才，并鼓励有价值的实习项目。

相关机构：NSC、DHS 和国会。

(3) 依据

①公共和私营部门在有限的范围内争夺经验丰富的网络专家，这造成网络安全领导力和专业知识匮乏。预计到 2022 年，合格网络人才的缺口将达到 180 万。

➤ 联邦政府提出的许多网络人才发展计划正按照第 13800 号总统行政令要求进行审核，建议政府将以上计划列为优先事项（详见附录 C）。

②联邦网络专家对特定私营部门系统了解不足，这限制了网络专家技术能力发挥，特别是在应对网络攻击时。实际上，我们需要整合来自行业和网络和运营系统专业知识，以形成合力应对网络攻击。

#### 建议 5

建立一套**具有时限的、以成果为导向的市场激励措施**，鼓励关键基础设施所有者和运营者升级其网络基础设施，投资发展最先进的技术，以符合行业标准或最佳实践要求。

(1) 激励措施包括：在例行满足行业标准情况下，减轻频繁的审计、报告和自我报告方面的监管要求；实施**具有时限的税收抵免政策**，激励企业升级安全系统；利用拨款或投资项目来支持升级或安全方面的投资，且不对企业提出具体升级目标。

(2) 要求私营部门实施国家标准和技术研究院（NIST）发布的《网络安全框架》，以使其获得联邦政府对其最关键资产的激励资格，并使私营部门认识到中小企业需要额外的支持才能满足其网络安全需求。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

(3) 依据。

①在网络世界中，攻击和防御变化快速、没有周期性，**网络规范的时效性相对滞后**，无法跟上风险的动态变化。

➤ 规范性要求导致我们仅重视合规性，而忽视了保持最佳的安全性。许多专家指出，规范只是一种有效的政府工具，目的是促进实现最低水平网络安全标准。

➤ 以成果为导向的激励措施可促使不同结构、规模和资源的公司灵活地实现或超越目标。

②以成果为导向的激励措施可以鼓励大规模的基础设施升级，充分利用公司资源达到卓越的安全性，而不仅仅是符合最低标准。

③NIST（网络安全框架）作为基础性文件，为网络安全提供了指南并明确了基本的最佳实践。

#### 建议 6

简化并显著加快对国家最关键的**网络资产所有者的安全许可审批**，提升敏感区域信息设施

(SCIF) 配置、可用性和易用性, 以确保获得安全许可的关键基础设施所有者和运营者可以在主要威胁或事件发生 1 小时内访问安全设施。

(1) 对于运营国家最关键网络资产(即一旦遭受攻击可能对公共安全、经济或国家安全造成灾难性影响的资产)的各个组织, 指导有关机构优先对组织中至少两名关键人员发放最高机密或敏感隔离信息(TS-SCI)许可。

(2) 完善许可流动制度: 由某一机构授予的许可应被其他机构认可, 当被授予许可的人员在机构间或向私营部门调动时, 支持其获得的许可跟随本人流动。

(3) 在全国范围内增加 SCIF 数量, 确保各机构维护的 SCIF 之间可以同步共享安全信息。

相关机构: DHS、ODNI、NSC、联邦调查局(FBI)、人事管理局以及其他所有颁发和提供 SCIF 支持的机构。

(4) 依据。

①尽管已有专门的私营部门许可计划, 但私营企业很少有恰当人员获得相应等级许可, 可在攻击发生时获得及时的网络威胁信息并采取行动。关键业务需要有至少两名获得许可的人员来应对潜在威胁。

②联邦政府的许可审批程序耗时久、效率低, 且私营部门很难通过。许可审批程序通常需要一年以上。

③联邦机构不轻易转让许可或认可由其他机构颁发的许可, 导致相关人员不得不重新开始漫长的许可申请程序。

➤ 许可看似与职位对应, 不随个人流动。如果持有许可的人员从一个机构到另一个机构工作或从联邦政府到私营部门工作, 其持有的许可不能随其流动, 必须重新申请相应许可。

➤ 这些低效、冗余的制度阻碍了已获得许可的人员保护关键企业的网络安全。

④如果私营部门人员不能迅速访问安全设施并接收关于网络威胁的敏感情报, 那么许可的价值将大打折扣。私营部门人员可能需要花费一个多小时才能访问 SCIF, 甚至可能需要飞到华盛顿亲自参加威胁信息发布会。快速变化的网络事件不会给信息共享预留这么久的时间。

## 建议 7

制定清晰的**网络威胁信息快速解密方案**, 主动与处于国家网络攻击防御前线的关键基础设施所有者和运营者分享网络威胁信息。

(1) 邀请最关键基础设施资产私营部门派遣获得许可的代表加入政府情报和信息共享中心, 协助通报及负责信息解密工作。

①考查被视为合署办公和信息共享典范的堪萨斯情报融合中心。持有 TS-SCI 级别许可的私营部门派员加入该融合中心工作, 积极与国民警卫队和其他机构代表合作, 共同处理网络问题。

②加大国家网络安全与通信集成中心(NCCIC)建设力度。该中心为协调公共和私营部门信息共享和响应、加强 ISAC 整合提供了平台。

(2) 扩大情报机构的使命, 要求情报机构主动与私营部门所有者和运营者共享情报信息, 以增强关键民用基础设施安全。建立相应方案, 要求情报分析人员和联邦响应官员在事件发生时, 尽快与持有许可的人员共享威胁信息或以解密方式传输。

相关机构: NSC、DHS、ODNI、FBI 和情报共同体(IC)。

（3）依据。

①无法快速解密并共享敏感级别不高的威胁信息（包括威胁迹象和脆弱性），导致私营企业在威胁事件发生前毫无准备。

- 那些急需了解威胁信息并立即保护关键系统的企业经常最后才知道威胁信息。
- 机密情报信息共享程序的设计是基于传播速度较慢的威胁，不足以应对不断升级的网络威胁。

②网络事件发生时，情报机构没有明确的责任或流程来主动解密信息，因为情报机构在历史上从未将私营企业视为其主要客户。

- 一方面，情报机构有能力解密和分享信息，但缺乏这样做的明确责任；另一方面，虽然国土安全部有明确责任与私营部门进行信息共享，但通常不掌握威胁信息，必须通过其他机构来解密和共享信息。

③建立相互信任关系是有效开展信息共享的核心。机构和企业必须将对方视为值得信赖的合作伙伴，积极主动地了解双方业务和信息需求，以保护国家免受网络威胁。

**建议 8**

**作为试点，成立由政府专家和电力、金融和通信行业专家组成的行动小组。**小组由拥有决策权的高级管理人员领导，配置资源，面对不断升级的网络威胁，从国家最高网络需求出发采取果断、快速、灵活的行动。

（1）组建三层架构的任务小组，包括：①拥有行政和资源配置能力的产业和政府高级管理人员；②解决实际问题和实现战略方向的业务管理人员；③来自行业 and 政府的负责深入研究和解决复杂问题的全职业务人员。该组织架构对任务小组的成功至关重要。

（2）通过 SICC 确定有意愿参加试点工作组的电力、金融服务和通信部门高级管理人员。

（3）将 NIAC 提出的建议和研究结果作为工作组的启动事项。任务小组应解决网络协调和信息共享的障碍，如法律和责任、数据隐私、机构碎片化、成本分摊等问题，以促进私营部门网络安全。

（4）从该试点中吸取经验教训，总结最佳实践，将任务小组协调方法推广到其他行业和关键基础设施企业。

相关机构：DOE、DHS、ODNI、NSC、SICC、国防部（DoD）、财政部和司法部（DOJ）。

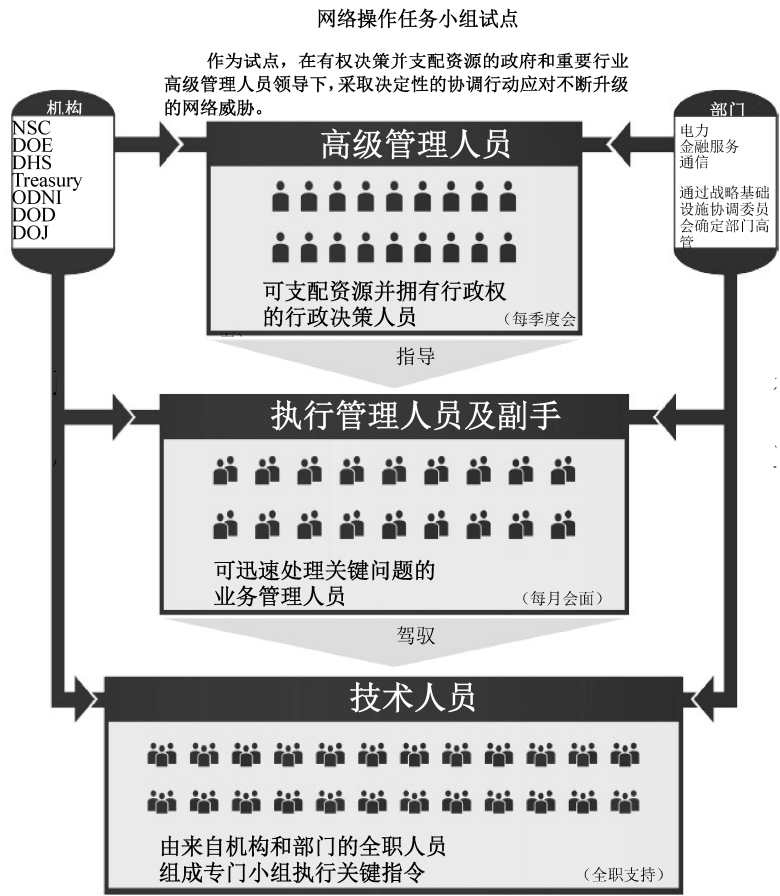
建议 8 设想提出了一种灵活的综合行动方法，我们认为这对于协调所有建议所需行动非常重要。后图展示了如何实施该设想。

（5）依据。

①当前，联邦网络安全能力、管理部门、使命、角色和监督的碎片化造成了应对网络威胁效率低下、配合不畅，亟需建立新方法。

②对于复杂网络问题的解决方案不能依靠单一机构来制定或主导。NIAC 明确了长期存在的基础性协调问题，需要重新研究如何调整机构任务并行使权力。在应对网络威胁时，我们需要行政领导力和战略方向。

③政府主要利益相关者必须全力支持私营部门的网络安全。高层领导应聚焦国家重要事项，建立明确事项，并指导跨部门业务小组以及公共和私营部门人员在应对网络威胁工作中取得进展。



➤ 运营任务小组将不再担当其他咨询委员会或其他被动协调小组，其使命将聚焦制定和实现解决方案。

④高级管理人员有能力确定战略方向和重点、配置资源并承担责任，因此对于实施行动至关重要。

⑤面对紧急威胁时，由各部门（即电力、金融服务和通信部门）高管代表组成的试点任务小组将迅速行动，着手解决最紧迫的问题，并对工作机制进行测试，以决定是否将该工作机制应用到其他部门。

➤ 电力、金融服务和通信部门的高级管理人员组成了战略基础设施协调委员会（SICC），代表行业参与政府活动和跨部门协调。

**建议 9**

计划于 2017 年 11 月举行国家级 GRIDEX IV 网络演习，测试联邦机构及职能在网络事件中的执行情况，并向具体机构提出针对性建议，以协调和明确联邦政府尚未明确的响应行动。

（1）邀请金融服务和通信部门的管理人员和代表参加演习计划。

（2）要求关键机构在演习之前编制白皮书，详细说明联邦政府如何在极端情况下支持响应。可以参考“国家网络事件响应计划”（NCIRP），该计划概述了响应的角色和责任，并确定了响应过程与方案之间的潜在差距。

（3）在演习中，要测试联邦决策、方案和流程，以提高联邦机构能力。例如，DHS 对如何在网络事件中利用《国防生产法》优化资源配置进行了大量研究。

（4）按照第 13800 号总统行政令要求，要利用该演习进一步验证和完善 DOE、DHS 和 DNI 评估结果，该结果将展现国家应对可造成长时间停电的重大网络事件的准备情况。

（5）根据 GridEx 演习形成的报告，向具体机构提出相关建议。行政机构应支持并为各机构提供相关资源，以实施这些建议。

相关机构：DOE、DHS、ODNI、NSC 和 SICC。

（6）依据。

①我们应对可造成关键基础设施严重物理破坏的大规模网络攻击的准备很可能不够充分。尽管已经从高层明确了负责网络事件响应的联邦机构，但联邦工作人员或关键基础设施所有者和运营者对响应的具体时间安排、流程和资源协调了解不足。

- 重大网络事件发生时，虽然一些机构设有相应的应急部门，但这些机构对于该做什么、怎么做以及由谁领导和行动时间等问题尚不清楚。
- NCIRP 对高级别网络事件响应角色进行了定义，但对触发联邦援助的事件类型及实践中存在的问题尚不清晰。

②网络事件响应的时间安排和资源需求与物理灾难响应有很大区别。为此必须制定和实施应对网络事件的详细政策、程序、联邦技术援助和互助方案。在沟通和协调中解决各类问题。

#### 建议 10

制定**最佳的网络安全治理方案**，整合不同联邦机构的资源和专业能力，以指导和协调国家网络防御。

（1）由网络任务小组（参见建议 8）评估其他国家的有效网络治理模型，推荐可以集中和提升网络治理能力的最佳方法，并为公共-私营部门网络防御提供国家层面协调。尽管美国的网络环境与其他国家不同，但我们认为如果美国政府高层可以更好地进行协调那么，将提升对联邦各机构的运营管理，帮助公共-私营部门针对网络威胁采取有效的响应行动。

（2）考虑建立一个高级职位或类似机构，以便对各联邦组织开展有效协调和运营管理演练。这需要国会采取行动，同时公众对网络威胁的紧迫性有广泛认可。根据经验，政府和民众在灾难性网络事件发生后才会真正意识到风险并采取行动。

相关机构：DHS、ODNI、NSC、DOJ 和 DoD。

（3）依据。

①联邦机构的能力和资源分散、重复，相互之间未能有效协同，不足以应对复杂的网络威胁。

- 各个机构承担着大量以任务为导向的专项工作。当前，美国拥有 6 个联邦网络安全中心、跨 20 个机构的 140 项网络机构和职能、4 个工具和 8 个评估项目。
- 这些数据凸显了当前问题的复杂性，也表明了在处理网络安全问题上，没有特别有效的解决方案。

②现有行政和立法体制导致大量机构和多个国会委员会拥有网络安全监督权，但对于国家应集中优先实施哪些行动形成的共识十分有限。

③创新的国家网络安全治理模式表明，实现快速有效的协调，需要由一个中央权威机构协

调国家网络优先事项，充分调动行业和政府资源，并为网络空间防御提供国家领导力。附录 D 总结了以色列和英国最新网络安全治理模式。

#### 建议 11

由国家安全顾问评估本报告提出的建议，并在 6 个月内召开政府高级官员会议，以扫清实施障碍，并明确下一步工作安排。

(1) 在 12 个月内，委托 NIAC 跟踪这些建议的执行情况，评估那些用以改善最关键基础设施资产的网络安全工作所取得的进展。

相关人员：国家安全顾问。

(2) 依据。

①现在迫切需要采取行动。历史上遭遇重大袭击或发生标志性事件（如“9·11”恐怖袭击）后，在公共需求和强烈政治意愿驱动下，战略性协调行动将会大有改进。在严重破坏关键服务的网络攻击发生前，我们有机会通过预见性和领导力，采取行动应对网络安全威胁。

②我们认为，诸如国家安全顾问等高级政府官员可利用其权威和领导力来召集政府机构负责人，与行业领袖们一道共同促进国家网络防御能力快速发展。

## 4. 目标：根本性改变

行动刻不容缓。我们国家需要从过去简单研究网络安全挑战转为采取有意义的战略举措，以增强国家网络安全，阻止重大网络攻击的发生。

工作组感谢政府对该研究中不断重申的关键问题持续关注，包括建立和维持网络工作小组，制定遏制网络侵略者的战略以及检查针对美国电力重大网络攻击的准备情况。

#### 国家愿景和领导

在高层领导支持下，我们建议制定一项国家战略，促进政府和行业发挥各自优势，成功阻止和抵御具有侵略性的网络攻击。我们需要明确短期和长期目标并最终实现国家愿景：

- 强有力的公众支持和政治意愿，推动网络安全成为国家首要任务。
- 来自最高级政府和私营部门的强有力领导。
- 联邦网络安全部门及其职能可在跨政府和私营部门间进行配合、协调并易于发挥作用。
- 企业可获得达到网络安全的基本标准的激励和技术援助。
- 针对网络事件，国家已做好有效抵御攻击、减轻攻击影响并快速响应和恢复的准备。
- 美国是世界网络安全的领导者。在公共-私营部门的通力协作下，美国在网络技术和人才队伍建设上将继续巩固世界领先地位。

我们国家需要明确方向和领导力来显著降低网络风险。NIAC 已做好准备在该领域继续为总统提供支持。

## 附录 A 研究方法

联邦政府和私营部门各自以及共同开展了大量的网络威胁检测工作。过去几年中，我们已

经完成一系列应对网络威胁的工作，如分析当前网络风险总体状况、行动的必要性以及需要采取哪些行动。

NIAC 的特有价值在于能够从重要私营部门所有者和运营者的角度出发，提供政府和私营部门充分协作的建议，以保护最关键的基础设施资产。

## 1. 任务来源

2017 年 5 月 11 日，第 13800 号总统行政令“加强联邦网络和关键基础设施的网络安全”发布。该行政令要求充分利用现有联邦职能来提高关键基础设施网络安全。2017 年 5 月 15 日，白宫通过 NSC 委托 NIAC 评估现有的联邦职能，并研究如何利用当前资源更好地保护最可能受到攻击的关键基础设施资产的网络安全。这些资产一旦遭到破坏，将在公共健康或安全、经济安全甚至国家安全方面对国家或区域产生灾难性影响。

## 2. 研究方法

为完成此项工作，NIAC 成立了一个由 9 名成员组成的网络研究工作组，该工作组对如何将现有联邦职能作用于私营部门进行了研究。为完成此项研究，工作组开展了以下工作：

（1）本研究工作基于 2017 年 2 月完成的 NIAC 网络调查研究。在早前研究中，研究小组采访了 20 多名前任及现任政府和私营部门的高级领导人，获得了 4 份机密简报和 4 份非机密简报，并研究了近期许多有关网络安全的战略和报告。本次研究印证了 NIAC 网络调查研究提出的 3 个紧急网络优先事项：

①对当前问题进行梳理分类。

- 针对当前关键基础设施面临的最严重的网络风险，采取即时和紧急修复措施。重点关注一旦遭到破坏将对美国经济和安全造成严重影响的行业及资产。
- 改善所有关键基础设施的网络安全状况，考虑提出相关合规性要求。
- 完善信息共享机制，实现机器到机器交换。

②制定提高网络韧性的新方法。

- 根据关键基础设施需求，研制安全的、有韧性的、能自我修复的新一代网络系统。制定新的解决方案，使攻击者很难突破关键基础设施的网络安全防护，从而不具有经济价值吸引力。

③加强公共-私营部门合作伙伴关系和领导能力。

- 制定有效的公共-私营部门领导层合作机制，强化应对重大网络事件和实施政策行动的领导力和有效决策力。
- 简化、更新和明确联邦政府内部的角色和职责。

（2）重点关注电力和金融服务的的前沿和极其重要的部门。NIAC 和国土安全咨询委员会（HSAC）等机构在报告中均认为这些部门支撑着其他关键基础设施部门的运营，对国家至关重要。因此，通过重点研究电力和金融部门得到的建议可以广泛适用于其他关键部门（详情见附录 C）。

（3）本次研究充分利用了现有信息并建立在其他大量的国家网络安全研究基础之上。例如，

我们借鉴了国家网络安全促进委员会（CENC）最新、最全面的报告“保护和发展数字经济”（2016 年 12 月发布）。CENC 由来自产业界、学术界和前政府的 12 名代表组成，该委员会提出了保护和发展数字经济的 6 项要求、16 项建议和 52 项具体行动。CENC 报告提出的建议涵盖了本次研究及其他研究提出的挑战，包括网络人才队伍发展建设、加强研究和发展，以及更好地了解联邦和私营部门在应对网络威胁中的角色和责任。

（4）明确行业网络需求，并着手考虑将联邦职能作用于私营部门。

（5）对 22 位政府和私营部门高级领导和专家进行访谈，包括在 NIAC 调查研究中采访过的 5 个人。在两项密切相关的研究中，工作组共采访了 38 位高级领导人和专家并将访谈内容作为研究基础。

（6）对涵盖 140 多个联邦机构及职能的综合数据集进行了评估，以确定这些联邦能力与行业需求，以及访谈和研究中强调的能力相符。

## 附录 B 致谢

略。

## 附录 C 关键部门面临网络威胁的紧迫性

鉴于本项研究的时间较短，工作组聚焦面临紧急威胁的部门，这些部门反映了国家关键基础设施面临网络挑战的复杂性和规模。电力和金融服务行业不仅相互关联，同时也是所有其他行业运行的基础。国土安全咨询委员会（HSAC）网络安全小组委员会在其 2016 年的报告中指出，由于其他行业对电力、金融服务和通信行业高度依赖，这 3 个行业面临的网络威胁增长。对以上 3 个部门的大规模网络攻击可导致多个部门的连锁效应，从而威胁公共卫生和安全、经济以及国家安全。

### 1. 网络攻击的复杂性和目的性不断增加

在过去 25 年中，发起攻击所需的技术知识不断减少。恶意网络工具和漏洞在互联网上很容易找到，并可被个人攻击者、有组织的犯罪和恐怖组织或国家利用。同时，网络攻击的复杂性也不断增加。例如，2010 年被首次发现的震网蠕虫病毒，通过一系列事件破坏了伊朗核设施：该恶意软件通过 USB 侵入到伊朗核设施 Windows 系统中，然后自主传播到核设施的可编程逻辑控制器中，最终摧毁了 984 个铀浓缩离心机。震网事件展示了成功入侵工业控制系统（ICS）的早期案例，并显示了可能造成的严重物理后果。

“专家们认为，网络威胁如此严重是因其进入门槛很低，而潜在回报巨大。”——NSA 法律总顾问 Glenn Gerstell，杜克大学法律、道德和国家安全中心 2017 年会议。

当前，不仅网络攻击变得更加复杂，即使发现了网络入侵行为，对其追踪溯源也十分困难。随着越来越多的设备启用网络功能或连接到网络，网络入侵数量不断增加。DHS 工业控制系统网络应急小组（ICS-CERT）在 2016 财年报告了 290 起针对关键基础设施控制系统的网络攻击。



在 2017 年 1 月出版的能源部《四年能源回顾》第二部分中指出：

“当前环境下，美国电网面临着遭受网络攻击的巨大风险，我们缺乏一系列具体行动和明确的政府部门响应和威胁通报机制。由网络攻击引起的大面积电力服务中断将对美国生命线网络、关键国防基础设施以及经济造成巨大破坏，并将威胁公民健康和平安。”

## 2. 通过网络攻击物理系统的能力

所有企业都面临着企业网络、客户账户、通信系统、网站和专有数据遭受网络攻击的威胁。然而，很多支撑电力、水、燃料以及化学制品的生成、处理和交付等物理过程控制或支撑通信和运输控制的关键基础设施企业的 OT 系统——通常被称为 ICS 或数据采集与监视控制系统（SCADA），面临着更深层次的威胁。针对 OT 系统的网络攻击可能破坏重要服务或关键设备，威胁人类健康和平安，并引发其他部门的混乱。

联网的 OT 设备提高了关键功能监测的自动化程度和效率，但也引入了新风险。通常，OT 平安（特别是电力部门的 OT 平安）依赖于物理隔离和专业性，以防止攻击者破坏正在运行的系统。每个设备的 OT 系统均按照其特定需求进行定制化生产，并只可与特定供应商的组件兼容。这些特性使攻击者不容易发现电力系统组件并对其实施攻击。

与中央 SCADA 或 IT 系统不同，OT 系统不会自动更新服务包、安装新版本和修复错误。实际上，由于物理隔离通常被认为是平安的，OT 设备中运行的软件通常与 10~15 年前相同。

### 运营技术 ≠ 信息技术

具有网络功能的感测和测量技术使关键系统更加可靠、自动化程度更高，但也产生了更多的漏洞，这就使得 OT 在以下方面与 IT 不同：

- OT 受到破坏可导致操作失效，破坏对客户的关键服务，并损坏高度专业化的设备。
- OT 处理网络事件的同时要维持关键功能的运行。
- 许多 OT 系统必须保证全天候实时运行，无法脱机进行修补或升级。
- OT 组件可能非常简单，没有足够的计算资源来支持额外的网络安全功能。
- OT 组件分布广泛、分散且可能位于公开访问的地方，容易遭受物理篡改。

升级、替换或修复网络组件可能会导致服务中断，即使是一个短暂的中断也会影响其他部门正常运行。当检测到攻击时，不能简单地将这些系统关闭。OT 平安技术在检测攻击的同时，还要维护系统功能不受影响。

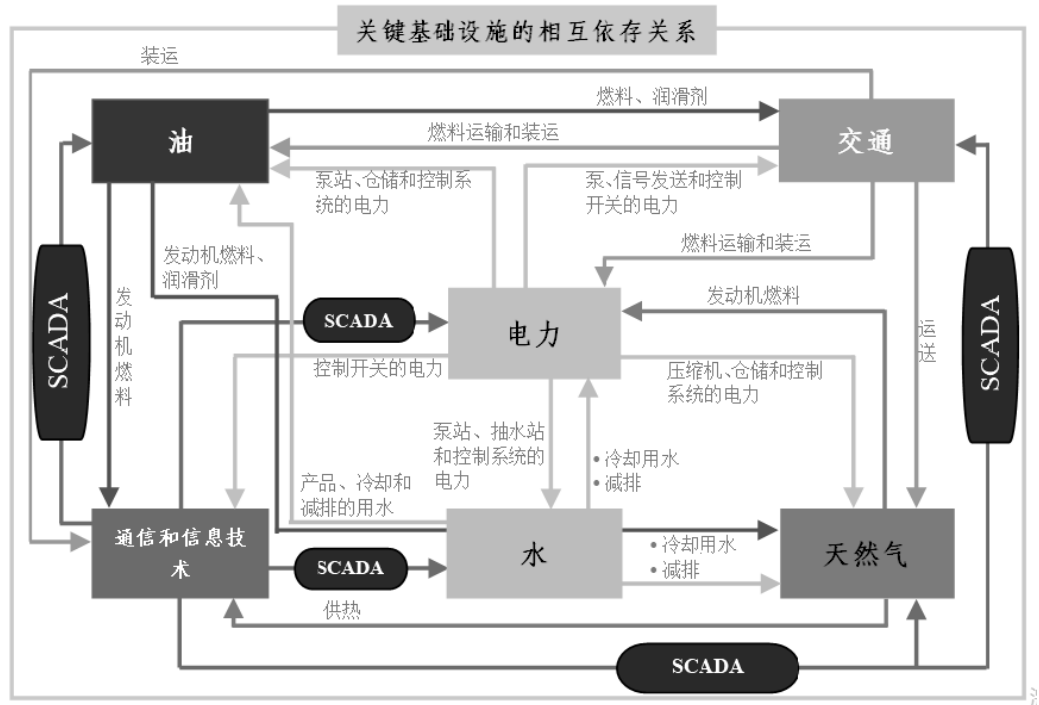
后图是与电力、能源、水利和运输部门业务密不可分的部门和 SCADA 控制系统之间的关联示意图。如果一个部门出现故障，那么它提供给其他部门的产品和服务也可能会受到干扰。

美国电力部门是一个由公共-私营企业及市政机构组成的混合体，包含 3300 多个设施，负责发电、输电和全国电力分配。这些系统相互连接，某个功能的中断可能会导致大范围且长时间的电力中断。

2015 年，一个重大网络攻击造成了乌克兰全国电力服务普遍中断，导致 22.5 万用户断电。在这次攻击中，乌克兰的 3 家配电公司和几个变电站均遭到恶意软件工具攻击。长期的策划和

协调配合使这次重大网络攻击得以成功实施.经调查,上述遭受攻击企业的系统在 9 个月前被网络钓鱼邮件攻陷。

这是针对输电行业的复杂网络攻击案例之一。针对电力部门的网络攻击除造成电力供应中断外,还将对价格昂贵的高度专业化设备造成破坏。系统或设备从故障状态恢复（特别是大容量电力系统）需要一个漫长的修复过程,这可能导致用户在相当长时间内处于黑暗中。



金融服务部门由投资机构、保险公司、信贷和融资组织,以及支撑这些业务的基础设施组成。这些组织包括从小型企业到跨国公司等各类机构,管理着数百万美元的资产。

2016 年,证券交易委员会主席认为网络安全是当前金融行业面临的<sup>1</sup>最大风险。同年晚些时候,孟加拉国央行的网络遭到入侵,黑客获取了全球银行间金融电信网络(SWIFT)的登录凭证。黑客通过访问支撑金融机构用来信息共享的 SWIFT 网络,窃取了超过 8000 万美元。

SWIFT 攻击显示了金融实体存在的固有风险,未来复杂的网络攻击可能会对经济产生更大规模、更长期的破坏。此类对主要金融机构数据的破坏行为将削弱消费者的信心。金融服务部门的中断也会对需要金融数据系统进行企业日常运营的其他部门产生附带影响。例如,2012 年,多家大型和小型金融机构遭受了分布式拒绝服务(DDoS 攻击)。

3. 定义和统一公共与私营部门角色

“尽管互联网在我们的生活中无处不在,但网络空间仍然是唯一这样的领域,要求私营企业必须在网络空间中保护自己,抵御来自某些国家的威胁。”——前商务部长 Penny Pritzker,在美国商会网络安全峰会上发表的主旨演讲,2016 年 9 月 27 日。

在美国历史上,我们为政府和私营部门确立了完善的角色来应对各类物理风险。例如,针

对导弹或炸弹袭击所产生的威胁，联邦政府指定了相关角色参与国家共同防御。针对类似规模的网络威胁，私营部门是国家第一道防线，而政府在保护关键系统中扮演的角色尚不明确。

普遍认为，保护美国免遭重大国家级攻击或可能对其公共安全、经济或国家安全造成影响 的攻击是联邦政府的责任。随着网络攻击的复杂性和影响面不断增加，传统的角色和责任变得模糊不清，特别是政府和行业应该共同承担的责任。应对网络攻击的难度和费用越来越高，私营企业需要更多的帮助和资源，这就需要政府发挥更大作用。而公共-私营双方如何发挥各自优势进行协调和共享是一项挑战。

在整个研究过程中，工作组多次听到有关“联邦政府应该行使权力威慑对手”的建议。作为一种外交手段，美国的确有足够的威慑力。我们必须寻找一种方法，将我们的威慑力延伸到网络空间，以警告对手不要轻举妄动。

联邦政府和私营部门一致认为，关键基础设施保护需要更多有技术和经验的网络人才队伍。未来几年，预计网络人才缺口将持续增加。网络安全中心预测到 2022 年，全球网络人才缺口将达到 180 万。

2016 年，联邦网络安全人才战略提出，在政府范围内建立一个四管齐下方法来增加网络安全就业机会，包括：通过教育和培训扩大网络人才队伍；加大招聘和宣传力度；利用更好的发展前景留住网络安全人才；明确当前网络安全人才需求数量。工作组通过访谈得知，有很多针对以上建议的项目正在实施，如国家科学基金会的网络部队服务奖学金、国防信息系统局发展计划以及网络安全职业和学习国家计划。

按照第 13800 号总统行政令要求，我们正对国家网络安全人才队伍和教育工作的范围及有效性进行评估。评估结果将于 2017 年晚些时候公布，工作组有意愿在国家网络安全人才队伍的发展和维护方面听取更多方面建议。

#### 4. 成功案例

涵盖 140 多个联邦政府及其职能的综合数据集展现了丰富的联邦现有能力，如联邦政府在网络防御和信息共享工作中扮演重要角色的能力。

##### （1）国家网络安全和通信整合中心（NCCIC）

NCCIC 提供了在联邦机构和私营机构之间的全方位、跨部门信息共享。NCCIC 包括 4 个分支机构：NCCIC 运营与整合（NO&I）、美国计算机应急准备小组（US-CERT）、工业控制系统网络应急响应小组（ICS-CERT）和国家通信协调中心（NCC）。

电力信息共享和分析中心（E-ISAC）和金融服务信息共享和分析中心（FS-ISAC）均派员加入 NCCIC，以更好地开展信息共享协作和协调。信息共享和分析中心（ISAC）通常被视为威胁信息共享以及政府与行业伙伴合作的成功机制。

##### （2）电力信息共享和分析中心（E-ISAC）

E-ISAC 是北美电力可靠性公司（NERC）的一个部门，负责收集和分析安全信息、协调事件管理以及与电力行业的利益相关者、跨行业部门和政府合作伙伴沟通威胁缓解策略。作为电力部门的主要安全沟通渠道，E-ISAC 与 DOE 和电力部门协调委员会（ESCC）合作，似增强电力部门准备和应对网络和物理威胁、漏洞和事件的能力。E-ISAC 的成功源于建立互相信任的伙伴关系。所有与 E-ISAC 共享的信息都受到联邦能源管理委员会（FERC）、NERC 及以法

律协议形式约束的合规落实计划，以及 NERC 公司政策以及 NERC 的物理和逻辑分离策略的保护。

### （3）金融服务信息共享和分析中心（FS-ISAC）

FS-ISAC 常被看作是会员之间信息共享的成功模式，其可向潜在受威胁企业提供各类信息来应对网络风险。FS-ISAC 在全球 30 多个国家拥有近 7000 名会员，包括银行、信用合作社、刷卡服务提供商、经纪商、第三方服务提供商和保险公司等。FS-ISAC 利用交通灯协议，按照信息类别共享不同等级信息。FS-ISAC 还致力于建立能源分析安全交换机制（EASE）。这一面向公共事业和能源电网的新情报共享共同体旨在为会员提供实时或准实时情报，帮助会员监控不断扩展的供应链并获取跨行业情报。

FS-ISAC 还致力于为对关乎国家和经济安全的金融机构组建具有针对性的特殊利益小组。通过这种方式，金融服务部门正在努力提高金融实体的网络能力、减少网络投入，并为加强与美国政府机构之间的沟通提供平台。最终，该小组可向金融服务领域之外扩展，让所有对国家和经济安全至关重要资产的所有者和运营者都参与进来。

### （4）网络安全风险信息共享计划（CRISP）

能源部的 CRISP 也被视为信息共享计划的成功案例之一。该计划旨在快速收集、分析并向参与方传播威胁信息。能源部及其国家实验室合作开发了用于捕捉网络数据的硬件设备，对来自能源部和情报共同体的数据进行自动收集和分析。分析结果将作为情报或威胁缓解措施发送给参与方。虽然硬件和分析能力最初在公共领域开发，但 CRISP 由 E-ISAC 负责管理和运营。该计划的成功在于它克服了最初遇到的来自私营-公共部门的障碍和阻力（如遵守隐私法、保密级别）。CRISP 成员为美国 75% 以上居民提供了电力服务。CRISP 机器到机器威胁信息共享平台也可以用于公司之间的信息共享。

## 附录 D 国家网络治理：英国和以色列模式

在访谈过程中，工作组多次听到“现有联邦机构及其网络能力未得到有效组织和使用”的声音。英国和以色列应对重大网络威胁和挑战的国家网络治理模式得到广泛认可，引发了其他国家的思考。我们对这两个国家的相关举措进行总结，得到以下 3 个重要结论，应由美国政府决定是否推动对网络职能的根本性重组：

- 中央政府成立了一个国家网络权威中心。
- 政府负责打击网络犯罪，包括开展追踪溯源、针对攻击者进行反击等，对网络对手形成威慑。
- 网络防御能力和网络技术领先密不可分。

### 1. 英国的网络工作举措

#### （1）国家网络安全战略 2016—2022

2016 年 11 月，英国公布了国家网络安全战略，旨在促进国家网络空间安全和韧性。该战略包括 3 个主要目标：一是抵御不断严峻的网络威胁，有效应对网络事件；二是阻止和破坏敌对活动，必要时采取有针对性的行动；三是发展网络安全产业、研发和人才培养。英国将为此

投资 19 亿英镑。

该战略明确英国政府负责保障国家网络的韧性，不允许因企业未采取必要的网络威胁防范措施而产生风险的情况出现。

## （2）国家网络安全中心（NCSC）

NCSC 于 2016 年 10 月启动，2017 年 2 月正式开放，该中心是英国网络安全空间监控、共享知识、解决系统漏洞及在重大国家安全问题上发挥领导作用的机构。NCSC 作为一个面向公众的组织，其前身可追溯到国家通信总局（GCHQ）。GCHQ 类似于美国 NSA，其功能是为相关方提供统一的威胁情报来源。

NCSC 取代了 3 个网络相关组织，包括网络评估中心（CCA）、英国计算机应急响应小组（CERT UK）和 CESG（GCHQ 的信息安全部门）。与网络有关的职责也从国家基础设施保护中心（CPNI）转移到 NCSC。

## （3）网络安全和信息保障办公室（OCSIA）

OCSIA 协助政府明确网络安全工作重点、提供战略方向以及协调政府网络安全计划。OCSIA 还支持网络安全教育和宣传相关活动，与私营部门合作交流信息并推动网络安全最佳实践，维护和改进国家网络安全能力。

## （4）规定

**《通用数据保护条例》：**该条例是一项欧盟法规，旨在加强和统一个人数据保护（包括传到欧盟以外的个人数据）。该条例将于 2018 年 5 月生效，并取代 1995 年发布的数据保护指令。该条例要求企业具备保护个人数据的能力，报告个人数据泄露事件并对违规未报情况进行罚款。信息专员办公室（ICO）和 NCSC 努力确保英国各组织在该条例的约束下，提高自身安全并不断发展。

**《网络和信息系统安全指令》（NIS 指令）：**该欧盟指令对高风险组织和数字服务提供商提出了网络防护的最低要求，以促使这些组织建立全面的网络风险管理计划。该指令旨在加强欧盟各国家在网络事件中的合作。

## 2. 以色列的网络工作举措

按照 2011 年第 3611 号政府决议，以色列成立了国家网络局，以提升国家网络空间能力。该局直接向总理报告，并为总理和政府提供指南和政策协调。第 3611 号决议还要求建立国家计算机应急响应小组（CERT）。国家网络局还负责促进学术界、产业界和政府部门合作，以加强国家关键基础设施的网络防御能力。

国家网络局有以下 4 项主要职能

- 防范网络威胁：制定国防防御战略，建立跨行业或行业规范；开展国家网络态势评估和网络威胁参考。
- 发展网络防御产业：建立网络研发计划，鼓励国际企业在以投资。
- 发展学术和人力资源：在以色列，网络安全人才培养正从一些私营企业向教育和培训拓展，鼓励年轻人从事网络安全方面工作。此举建立在注重安全的国家文化基础之上，全社会对网络威胁的紧迫性和重要性达成共识。
- 国际合作：与网络目标相似的国家建立合作关系，促进信息共享、研发等。

2015 年,第 2444 号决议获批,以色列成立了**国家网络防御局 (NCDA)**。该决议要求国家网络局重点负责战略制定,NCDA 则将工作重点放在增强网络防护。

NCDA 的宗旨是在网络空间中负责国家层面的指挥、运行和实施一切必要的防御和操作,以对网络攻击进行全面和持续的防御,包括实时处理网络威胁和网络事件、开展当前网络态势评估、收集和研究情报,以及与专门机构开展合作。

对以色列网络安全组织改革的批评主要集中在角色和责任不清。这些批评主要来自于以色列其他安全机构的负责人以及以色列议会外交和国防委员会发布的一份报告。

由于国家网络管理部门隶属于国家网络局,有这种担心,该组织架构可能妨碍政府改善和提高民间团体的网络安全防御能力。

议会报告中引用的其他结论包括:政府应避免成为另一个情报收集机构;政府发布的任何法律法规必须考虑所有国防和民间团体的意见;每 5 年应进行重新审查网络领导的组织架构。

## 附录 E 参考文献

- [1] Adamsky, Dmitry. The Israeli Odyssey toward its National Cyber Security Strategy. *The Washington Quarterly* 40, no. 2:113-127. June 14, 2017. [https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ\\_Summer2017\\_Adamsky.pdf](https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ_Summer2017_Adamsky.pdf).
- [2] Alkhalisi, Zahraa. Saudi Arabia warns of new crippling cyber attack. CNN, January 26, 2017. <http://money.cnn.com/2017/01/25/technology/saudi-arabia-cyber-attack-warning/>.
- [3] Atlantic Council. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures. September 2015. <http://publications.atlanticcouncil.org/cyber risks/>.
- [4] Behr, Peter and Blake Sobczak. White House-New cyber order draft keeps focus on critical grid companies. *E&E News*, May 4, 2017. <https://www.eenews.net/energywire/2017/05/04/stories/1060054017>.
- [5] Bell, Greg, Tony Buffomante, Ken Dunbar, and Cliff Justice. Technology: AI Adds a New Layer to Cyber Risk. *Harvard Business Review*, April 13, 2017. <https://hbr.org/2017/04/ai-adds-a-new-layer-to-cyber-risk>.
- [6] Boyd, Aaron. Civilian Cybersecurity Strategy coming this summer. *Federal Times*, July 14, 2015. <http://www.federaltimes.com/story/government/cybersecurity/2015/07/14/civilian-cybersecurity-strategy/30138103/>.
- [7] Boyd, Aaron. Initial meeting lays out how commission will enhance cybersecurity. *Federal Times*, April 15, 2016. <http://www.federaltimes.com/story/government/cybersecurity/2016/04/15/cyber-commission-first-meeting/83080592/>.
- [8] Brown, Jared T. Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress. Congressional Research Service. October 21, 2011. <https://fas.org/sgp/crs/homsec/R42073.pdf>.
- [9] Burley, Diana L. Testimony Before the United States of Representatives Committee on Science, Space, & Technology, Subcommittee on Research and Technology Hearing on Strengthening U.S. Cybersecurity Capabilities. February 14, 2017. <http://docs.house.gov/meetings/SY/SY15/>

- 20170214/105554/HHRG-115-SY15-Wstate-BurleyD-20170214.pdf.
- [10] Carberry, Sean D. Fate of Trump cyber order still unclear. FCW: The Business of Federal Technology, April 11, 2017. <https://fcw.com/articles/2017/04/11/trump-cyber-order-murky.aspx>.
  - [11] Center for Cyber Safety and Education. Global Information Security Workforce Study. 2017. [https://iamcybersafe.org/research\\_millennials/](https://iamcybersafe.org/research_millennials/).
  - [12] Center for Strategic and International Studies (CSIS). CSIS Cyber Policy Task Force. Accessed January 13, 2017. <https://www.csis.org/programs/technology-policy-program/cybersecurity/csis-cyber-policy-task-force>.
  - [13] Center for Strategic and International Studies (CSIS). From Awareness to Action. A Cybersecurity Agenda for the 45th President. Accessed July 18, 2017. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110\\_Lewis\\_CyberRecommendationsNextAdministration\\_Web.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf).
  - [14] Center for Strategic and International Studies (CSIS). Significant Cyber Incidents List. Accessed July 18, 2017. [https://csis-prod.s3.amazonaws.com/s3fs-public/170519\\_Significant\\_Cyber\\_Events\\_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39](https://csis-prod.s3.amazonaws.com/s3fs-public/170519_Significant_Cyber_Events_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39).
  - [15] Center for Strategic and International Studies (CSIS) Cyber Policy Task Force. Testimony of Iain Mulholland. Strengthening U.S. Cybersecurity Capabilities. February 14, 2017. <http://docs.house.gov/meetings/SY/SY15/20170214/105554/HHRG-115-SY15-Wstate-MulhollandI-20170214.pdf>.
  - [16] Center for Strategic and International Studies (CSIS) Cybersecurity Commission. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. November 2010. [https://csis-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/101111\\_Evans\\_HumanCapital\\_Web.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf).
  - [17] Center for Strategic and International Studies (CSIS) Cybersecurity Commission. Cybersecurity Two Years Later. 2011. <https://www.csis.org/analysis/cybersecurity-two-years-later>.
  - [18] Center for Strategic and International Studies (CSIS) Cybersecurity Commission. Securing Cyberspace for the 44th Presidency. 2008. [https://csis-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/media/csis/pubs/081208\\_securingcyberspace\\_44.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf).
  - [19] NIAC Pre-Decisional 37.
  - [20] Center for Strategic and International Studies (CSIS) Cybersecurity Commission. Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines. 2009. [https://csis-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/Twenty\\_Critical\\_Controls\\_for\\_Effective\\_Cyber\\_Defense\\_CAG.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf).
  - [21] Chachko, Elena. Cyber Reform in Israel at an Impasse: A Primer. Lawfare, April 27, 2017. <https://www.lawfareblog.com/cyber-reform-israel-impasse-primer>.
  - [22] Chappell, Bill. We're No. 3: U.S. Infrastructure, Education Faulted In Global Competitiveness Index. NPR, September 28, 2016. <http://www.npr.org/sections/thetwo-way/2016/09/28/49579>

- 6271/were-no-3-u-s-infrastructure-education-faulted-in-global-competitiveness-index.
- [23] Columbus, Louis. Roundup of Internet of Things Forecasts and Market Estimates. Forbes, November 27, 2016. <https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#6c7f7dc2292d>.
  - [24] Commission on Enhancing National Cybersecurity (CENC). Briefing on Current Federal Initiatives for the Federal Governance Sub-Committee. Washington, D.C. August 3, 2016. [https://www.nist.gov/sites/default/files/documents/2017/01/19/commission\\_preparatory\\_working\\_group\\_meeting\\_august\\_3\\_2016\\_clean\\_final.pdf](https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_august_3_2016_clean_final.pdf).
  - [25] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. American University Washington College of Law, Washington, D.C. September 19, 2016. [https://www.nist.gov/sites/default/files/documents/2016/11/15/sept\\_19\\_2016\\_amer\\_univ\\_meeting\\_minutes.pdf](https://www.nist.gov/sites/default/files/documents/2016/11/15/sept_19_2016_amer_univ_meeting_minutes.pdf).
  - [26] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. Conference Calls. July 7, 2016 – November 21, 2016.
  - [27] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. New York University School of Law-Vanderbilt Hall, New York, NY. May 16, 2016. [https://www.nist.gov/sites/default/files/may\\_16\\_2016\\_nyc\\_meeting\\_minutes.pdf](https://www.nist.gov/sites/default/files/may_16_2016_nyc_meeting_minutes.pdf).
  - [28] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. University of California, Berkeley, Berkeley, CA. June 21, 2016. [https://www.nist.gov/sites/default/files/june\\_21\\_2016\\_ucb\\_meeting\\_minutes.pdf](https://www.nist.gov/sites/default/files/june_21_2016_ucb_meeting_minutes.pdf).
  - [29] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. University of Houston, Houston, TX. July 14, 2016. [https://www.nist.gov/sites/default/files/commission\\_on\\_enhancing\\_national\\_cybersecurity\\_mn\\_09072016.pdf](https://www.nist.gov/sites/default/files/commission_on_enhancing_national_cybersecurity_mn_09072016.pdf).
  - [30] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. University of Minnesota, Minneapolis, MN. August 23, 2016. [https://www.nist.gov/sites/default/files/documents/2016/11/15/aug\\_23\\_2016\\_univ\\_minnesota\\_meeting\\_minutes.pdf](https://www.nist.gov/sites/default/files/documents/2016/11/15/aug_23_2016_univ_minnesota_meeting_minutes.pdf).
  - [31] Commission on Enhancing National Cybersecurity (CENC). Meeting Minutes. U.S. Department of Commerce-Commerce Research Library, Washington, D.C. April 14, 2016. [https://www.nist.gov/sites/default/files/documents/cybercommission/Meeting\\_Minutes\\_April\\_14.pdf](https://www.nist.gov/sites/default/files/documents/cybercommission/Meeting_Minutes_April_14.pdf).
  - [32] Commission on Enhancing National Cybersecurity (CENC). Panelist Statements. New York University—School of Law, New York, NY. May 16, 2016. [https://www.nist.gov/sites/default/files/may\\_16\\_panelist\\_statements.pdf](https://www.nist.gov/sites/default/files/may_16_panelist_statements.pdf).
  - [33] Commission on Enhancing National Cybersecurity (CENC). Panelist Statements. University of California, Berkeley, Berkeley, CA. June 21, 2016. [https://www.nist.gov/sites/default/files/documents/2016/09/12/june21\\_panelist\\_statements.pdf](https://www.nist.gov/sites/default/files/documents/2016/09/12/june21_panelist_statements.pdf).
  - [34] Commission on Enhancing National Cybersecurity (CENC). Panelist and Speaker Statements” University of Houston, Houston, TX. July 14, 2016. [https://www.nist.gov/sites/default/files/july14\\_panelist\\_statements.pdf](https://www.nist.gov/sites/default/files/july14_panelist_statements.pdf).



- [35] Commission on Enhancing National Cybersecurity (CENC). Panelist and Speaker Statements. University of Minnesota, Minneapolis, MN. August 23, 2016. [https://www.nist.gov/sites/default/files/documents/2016/08/25/august23\\_panelist\\_statements.pdf](https://www.nist.gov/sites/default/files/documents/2016/08/25/august23_panelist_statements.pdf).
- [36] Commission on Enhancing National Cybersecurity (CENC). Panelist and Speaker Statements. American University, Washington, D.C. September 19, 2016. [https://www.nist.gov/sites/default/files/documents/2016/09/23/dc\\_commission\\_panelist\\_and\\_speaker\\_statements.pdf](https://www.nist.gov/sites/default/files/documents/2016/09/23/dc_commission_panelist_and_speaker_statements.pdf).
- [37] NIAC Pre-Decisional 38.
- [38] Commission on Enhancing National Cybersecurity (CENC). Preparatory Working Group Meeting. Washington D.C. October 19, 2016. [https://www.nist.gov/sites/default/files/documents/2017/01/19/commission\\_preparatory\\_working\\_group\\_meeting\\_october\\_19\\_2016\\_clean\\_final.pdf](https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_october_19_2016_clean_final.pdf).
- [39] Commission on Enhancing National Cybersecurity (CENC). Recommendations Working Group Discussion. Washington, D.C. November 8, 2016. [https://www.nist.gov/sites/default/files/documents/2017/01/19/commission\\_preparatory\\_working\\_group\\_meeting\\_november\\_8\\_2016\\_clean\\_final.pdf](https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_november_8_2016_clean_final.pdf).
- [40] Commission on Enhancing National Cybersecurity (CENC). Report on Securing and Growing the Digital Economy. December 2016. <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>.
- [41] Dahan, Maha El, Jim Finkle, Andrew Hay, Mark Potter, and Reem Shamseddine. Saudi Arabia warns on cyber defense as Shamoon resurfaces, Reuters, January 23, 2017. <http://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR>.
- [42] Defense Information Systems Agency (DISA). Pathways Program. Accessed July 31, 2017. <http://www.disa.mil/careers/pathways-program>.
- [43] Deloitte. Quantum Dawn 2: A simulation to exercise cyber resilience and crisis management capabilities. October 21, 2013. <http://www.sifma.org/uploadedfiles/services/bcp/after-actionreport2013.pdf?n=96397>.
- [44] Deloitte. Standing Together for Financial Industry Resilience: Quantum Dawn 3 After-Action Report. November 19, 2015. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-quantum-dawn-3-after-action-report.pdf>.
- [45] Electricity Information Sharing and Analysis Center (E-ISAC). About E-ISAC. Accessed July 28, 2017. <https://www.eisac.com/#about>.
- [46] Electricity Information Sharing and Analysis Center (E-ISAC). Analysis of the Cyber Attack on the Ukrainian Power Grid. March 18, 2016. [http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- [47] Electricity Information Sharing and Analysis Center (E-ISAC). E-ISAC Brochure. Public Document Library. June 2017. <https://www.eisac.com/api/documents/6436/publicdownload>.
- [48] Electricity Subsector Coordinating Council (ESCC). ESCC Initiatives. March 2017. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.6>.
- [49] European Commission. Digital Single Market: The Directive on security of network and

- information systems (NIS Directive). Accessed July 17, 2017. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.
- [50] Even, Shmuel, David Siman-Tov, and Gabi Siboni. Structuring Israel's Cyber Defense. Institute for National Security Studies with Tel Aviv University. INSS Insight No. 856. September 21, 2016. <http://www.inss.org.il/publication/structuring-israels-cyber-defense/>.
- [51] Executive Office of the President. Federal Cybersecurity Research and Development Strategic Plan. Cybersecurity National Action Plan. 2016. [https://www.cerias.purdue.edu/assets/symposium/2016/docs/shannon\\_slides.pdf](https://www.cerias.purdue.edu/assets/symposium/2016/docs/shannon_slides.pdf).
- [52] Executive Office of the President. National Science and Technology Council. Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program. December 2011. [https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed\\_Cybersecurity\\_RD\\_Strategic\\_Plan\\_2011.pdf](https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf).
- [53] Executive Office of the President. Office of Management and Budget. Memorandum for the Heads of Executive Departments and Agencies: Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 19, 2017. <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf>.
- [54] Executive Office of the President. President's Council of Advisors on Science and Technology. Report to the President Immediate Opportunities For Strengthening The Nation's Cybersecurity. November 2013. <https://www.broadinstitute.org/files/sections/about/PCAST/2013%20pcast-cybersecurity.pdf>.
- [55] Fattah, Zainab. Cyber Attacks Target Saudi Arabia's State Agencies, Companies, Bloomberg, January 24, 2017. <https://www.bloomberg.com/news/articles/2017-01-24/cyber-attacks-target-saudi-arabia-s-state-agencies-companies>.
- [56] Federal Energy Regulatory Commission (FERC). Commission Will Approve Applications For Prudent Cost Recovery Tied To Security Needs. Press release, September 14, 2001. <https://www.ferc.gov/media/news-releases/2001/2001-3/nr01-38.PDF>.
- [57] NIAC Pre-Decisional 39.
- [58] Financial Services Information Sharing and Analysis Center (FS-ISAC). 2017 FS-ISAC Annual Summit. Agenda. May 1, 2017. <https://www.fsisac-summit.com/files/galleries/2017annual-web-descriptions.pdf>.
- [59] Financial Services Information Sharing and Analysis Center (FS-ISAC). FS-ISAC Launches New Energy Sector Sharing Community. Press release, February 15, 2017. [https://www.fsisac.com/sites/default/files/news/FS-ISAC\\_Sector\\_EASE\\_Press\\_Release\\_FINAL\\_2-15-17.pdf](https://www.fsisac.com/sites/default/files/news/FS-ISAC_Sector_EASE_Press_Release_FINAL_2-15-17.pdf).
- [60] Financial Services Information Sharing and Analysis Center (FS-ISAC). Strength In Sharing: 2017 FS-ISAC Annual Summit Brochure. 2017. <https://www.fsisac-summit.com/files/galleries/2017annual-brochure.pdf>.
- [61] Flournoy, Michele and Amy Schafer. Building a cyber ROTC, Boston Globe, July 13, 2017.

- <https://www.bostonglobe.com/opinion/2017/07/12/flournoy/RZJgYqcmIScy51HyUiopII/story.html>.
- [62] Fowke, Benjamin G.S. III. Testimony before the U.S. Senate Committee on Energy and Natural Resources Subcommittee on Energy hearing to Examine Cybersecurity Threats to the U.S. Electrical Grid and Technology Advancements to Minimize the Threat. March 28, 2017. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=40A50EA7-75FA-4CEB-9A5A-3FE9074F4B77](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=40A50EA7-75FA-4CEB-9A5A-3FE9074F4B77).
- [63] Franzetti, Andres. In the Lane Duck, How Congress Makes Cybersecurity A Non-Partisan Priority. Forbes. November 14, 2016. <http://www.forbes.com/sites/realspin/2016/11/14/in-the-lame-duck-how-congress-makes-cybersecurity-a-non-partisan-priority/#5920c93b3654>.
- [64] Friedman, Sam and Adam Thomas. Demystifying cyber insurance coverage, Deloitte University Press, February 23, 2017. <https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html>.
- [65] Gambrell, Jon. Saudi Arabia warns destructive computer virus has returned (Updated), Phys Org News, January 24, 2017. <https://phys.org/news/2017-01-saudi-arabia-destructive-virus.html>.
- [66] Gerstell, Glenn. Confronting the Cybersecurity Challenge—Keynote Address by Glenn S. Gerstell, NSA General Counsel. 2017 Law, Ethics and National Security Conference at Duke Law School. February 25, 2017. <https://www.nsa.gov/news-features/speeches-testimonies/speeches/20170225-gerstell-duke-keynote.shtml>.
- [67] Gregory-Brown, Bengt. Securing Industrial Control Systems—2017. SANS Institute. June 2017.
- [68] HM Government. Cyber Security Regulation and Incentives Review. December 2016. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/579442/Cyber\\_Security\\_Regulation\\_and\\_Incentives\\_Review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf).
- [69] HM Government. Office of Cyber Security and Information Assurance. Accessed July 7, 2017. <https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance>.
- [70] HM Government. National Cyber Security Centre. Accessed July 7, 2017. <https://www.ncsc.gov.uk/about-us>.
- [71] HM Government. National Cyber Security Strategy 2016-2022. 2016. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/567242/national\\_cyber\\_security\\_strategy\\_2016.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf).
- [72] HM Government Information Commissioner's Office. Overview of the General Data Protection Regulation. Accessed July 17, 2017. <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>.
- [73] Homeland Security Advisory Council (HSAC). Final Report of the Cybersecurity Subcommittee, Part I: Incident Response. June 2016. [https://www.dhs.gov/sites/default/files/publications/HSAC\\_Cybersecurity\\_IR\\_FINAL\\_Report.pdf](https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf).
- [74] House of Representatives. National Defense Authorization Act for Fiscal Year 2017.

- November 2016. <http://docs.house.gov/billsthisweek/20161128/CRPT-114HRPT-S2943.pdf>.
- [75] Idaho National Laboratory. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. August 2016. <https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector>.
- [76] IBM Global Technology Services. IBM Security Services 2014 Cyber Security Intelligence Index. 2014. [https://media.scmagazine.com/documents/82/ibm\\_cyber\\_security\\_intelligence\\_20450.pdf](https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligence_20450.pdf).
- [77] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). About the Industrial Control Systems Cyber Emergency Response Team. Accessed July 24, 2017. <https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>.
- [78] NIAC Pre-Decisional 40.
- [79] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT Annual Assessment Report FY 2016. Accessed July 19, 2017. [https://ics-cert.us-cert.gov/sites/default/files/Annual\\_Reports/FY2016\\_Industrial\\_Control\\_Systems\\_Assessment\\_Summary\\_Report\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf).
- [80] Clinton, Larry, and David Perera, eds. The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity. Internet Security Alliance. September 2016.
- [81] Israeli Government. Resolution No. 3611 of the Government of August 7, 2011: Advancing National Cyberspace Capabilities. Accessed July 17, 2017. <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>.
- [82] Israeli Prime Minister's Office. Mission of the Bureau. Accessed July 17, 2017. <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx>.
- [83] Intelligence and National Security Alliance (INSA). FINnet: A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing. June 2017. <https://www.insonline.org/wp-content/uploads/2017/06/INSA-FINnet-Proposal-June-2017.pdf>.
- [84] The Knesset. Foreign Affairs and Defense Committee: National Cyber Defense Authority should be in charge of Israel's cyber defense. Press release, August 1, 2016. [https://knesset.gov.il/spokesman/eng/PR\\_eng.asp?PRID=12198](https://knesset.gov.il/spokesman/eng/PR_eng.asp?PRID=12198).
- [85] Lambert, Lisa, and Suzanne Barlyn. SEC says cyber security biggest risk to financial system, Reuters, May 17, 2016. <http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4>.
- [86] Lloyd's. Business Blackout. July 2015. <https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout>.
- [87] Madnick, Stuart. Preparing for the Cyber attack That Will Knock Out U.S. Power Grids, Harvard Business Review, May 10, 2017. <https://hbr.org/2017/05/preparing-for-the-cyber-attack-that-will-knock-out-u-s-power-grids>.
- [88] Mandiant Consulting. Threat Landscape: By The Numbers. Infographic, August 10, 2016.

- <https://www.slideshare.net/FireEyeInc/infographic-mtrends-2016>.
- [89] National Cybersecurity and Communications Integration Center (NCCIC). NCCIC. Accessed July 28, 2017. <https://www.us-cert.gov/nccic>.
  - [90] National Cybersecurity and Communications Integration Center (NCCIC). Preparing for Cyber Incident Analysis. Accessed July 18, 2017. [https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT\\_FactSheet\\_Cyber\\_Incident\\_Analysis\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Cyber_Incident_Analysis_S508C.pdf).
  - [91] National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT Fact Sheet. Accessed July 19, 2017. [https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT\\_FactSheet\\_IR\\_Pie\\_Chart\\_FY2016\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf).
  - [92] National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT: Year in Review 2016. Accessed July 18, 2017. [https://ics-cert.us-cert.gov/sites/default/files/Annual\\_Reports/Year\\_in\\_Review\\_FY2016\\_Final\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf).
  - [93] National Cybersecurity Center of Excellence (NCCoE). Fact Sheet: About the National Cybersecurity Center of Excellence. Accessed July 18, 2017. <https://nccoe.nist.gov/sites/default/files/library/fact-sheets/nccoe-fact-sheet.pdf>.
  - [94] National Infrastructure Advisory Council (NIAC). A Framework for Establishing Critical Infrastructure Resilience Goals. 2010. <https://www.dhs.gov/sites/default/files/publications/niac-framework-establishing-resilience-goals-final-report-10-19-10-508.pdf>.
  - [95] National Infrastructure Advisory Council (NIAC). Best Practices for Government to Enhance the Security of National Critical Infrastructure. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-best-practices-ci-security-final-report-04-13-04-508.pdf>.
  - [96] National Infrastructure Advisory Council (NIAC). Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce. 2008. <https://www.dhs.gov/sites/default/files/publications/niac-chemical-biological-radiological-final-report-01-08-08-508.pdf>.
  - [97] National Infrastructure Advisory Council (NIAC). Clarifications on Executive Collaboration for the Nation's Strategic Infrastructure: Responses to National Security Council Questions. 2015. <https://www.dhs.gov/sites/default/files/publications/niac-ceo-report-response-nsc-final-12-01-15-508.pdf>.
  - [98] NIAC Pre-Decisional 41.
  - [99] National Infrastructure Advisory Council (NIAC). Common Vulnerability Scoring System. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-common-vulnerability-scoring-final-report-10-12-04-508.pdf>.
  - [100] National Infrastructure Advisory Council (NIAC). Convergence of Physical and Cyber Technologies and Related Security Management Challenges. 2007. <https://www.dhs.gov/sites/default/files/publications/niac-physical-cyber-final-report-01-16-07-508.pdf>.
  - [101] National Infrastructure Advisory Council (NIAC). Critical Infrastructure Partnership Strategic Assessment. 2008. <https://www.dhs.gov/sites/default/files/publications/niac-ci-partnership-assessment-final-report-10-14-08-508.pdf>.
  - [102] National Infrastructure Advisory Council (NIAC). Critical Infrastructure Resilience. 2009.

- <https://www.dhs.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf>.
- [103] National Infrastructure Advisory Council (NIAC). Critical Infrastructure Security Resilience National Research and Development Plan. 2014. <https://www.dhs.gov/sites/default/files/publications/NIAC-CISR-RD-Plan-Report-Final-508.pdf>.
  - [104] National Infrastructure Advisory Council (NIAC). Cross Sector Interdependencies and Risk Assessment Guidance. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-interdependencies-risk-assess-final-report-01-13-04-508.pdf>.
  - [105] National Infrastructure Advisory Council (NIAC). Cyber Scoping Study Working Group Quarterly Business Meeting Presentation. February 16, 2017.
  - [106] National Infrastructure Advisory Council (NIAC). Evaluation and Enhancement of Information Sharing and Analysis. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-eval-enhance-info-sharing-final-report-07-13-04-508.pdf>.
  - [107] National Infrastructure Advisory Council (NIAC). Executive Collaboration for the Nation's Strategic Infrastructure. 2015. <https://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf>.
  - [108] National Infrastructure Advisory Council (NIAC). Framework for Dealing with Disasters and Related Interdependencies. 2009. <https://www.dhs.gov/sites/default/files/publications/niac-framework-dealing-disasters-final-report-07-14-09-508.pdf>.
  - [109] National Infrastructure Advisory Council (NIAC). Hardening the Internet. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-hardening-internet-final-report-10-12-04-508.pdf>.
  - [110] National Infrastructure Advisory Council (NIAC). Implementation of EO 13636 and PPD-21. 2013. <https://www.dhs.gov/sites/default/files/publications/niac-eo-ppd-implement-final-report-11-21-13-508.pdf>.
  - [111] National Infrastructure Advisory Council (NIAC). The Insider Threat to Critical Infrastructures. 2008. <https://www.dhs.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf>.
  - [112] National Infrastructure Advisory Council (NIAC). Intelligence Information Sharing Report. 2012. <https://www.dhs.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12-508.pdf>.
  - [113] National Infrastructure Advisory Council (NIAC). Optimization of Resources for Mitigating Infrastructure Disruptions. 2010. <https://www.dhs.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf>.
  - [114] National Infrastructure Advisory Council (NIAC). The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States. 2007. <https://www.dhs.gov/sites/default/files/publications/niac-pandemic-outbreak-final-report-01-17-07-508.pdf>.
  - [115] National Infrastructure Advisory Council (NIAC). Prioritizing Cyber Vulnerabilities. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-cyber-vulnerabilities-final-report-10->

- 12-04-508.pdf.
- [116] National Infrastructure Advisory Council (NIAC). Public-Private Sector Intelligence Coordination. 2006. <https://www.dhs.gov/sites/default/files/publications/niac-intelligence-coordination-final-report-07-11-06-508.pdf>.
  - [117] National Infrastructure Advisory Council (NIAC). Risk Management Approaches to Protection. 2005. <https://www.dhs.gov/sites/default/files/publications/niac-risk-management-final-report-10-11-05-508.pdf>.
  - [118] National Infrastructure Advisory Council (NIAC). Sector Partnership Model Implementation. 2005. <https://www.dhs.gov/sites/default/files/publications/niac-sector-partnership-implem-final-report-10-11-05-508.pdf>.
  - [119] NIAC Pre-Decisional 42.
  - [120] National Infrastructure Advisory Council (NIAC). Strengthening Regional Resilience. 2013. <https://www.dhs.gov/sites/default/files/publications/niac-regional-resilience-final-report-11-21-13-508.pdf>.
  - [121] National Infrastructure Advisory Council (NIAC). Transportation Sector Resilience. 2015. <https://www.dhs.gov/sites/default/files/publications/niac-transportation-resilience-final-report-07-10-15-508.pdf>.
  - [122] National Infrastructure Advisory Council (NIAC). Vulnerability Disclosure Framework. 2004. <https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf>.
  - [123] National Infrastructure Advisory Council (NIAC). Water Sector Resilience. 2016. <https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf>.
  - [124] National Infrastructure Advisory Council (NIAC). Workforce Preparation, Education and Research. 2006. <https://www.dhs.gov/sites/default/files/publications/niac-workforce-education-final-report-04-11-06-508.pdf>.
  - [125] National Initiative for Cybersecurity Careers and Studies (NICCS). NICCS Workforce Development. Accessed July 31, 2017. <https://niccs.us-cert.gov/workforce-development>.
  - [126] National Initiative for Cybersecurity Education (NICE). NICE Webinar Series. The President's Executive Order on Cybersecurity Workforce: Next Steps and How to Engage. June 5, 2017. [https://www.nist.gov/sites/default/files/documents/2017/07/05/cybersecurity\\_eo\\_webinar\\_slides.pdf](https://www.nist.gov/sites/default/files/documents/2017/07/05/cybersecurity_eo_webinar_slides.pdf).
  - [127] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.
  - [128] National Institute of Standards and Technology (NIST). National Initiative for Cybersecurity Education (NICE), About. Accessed July 31, 2017. <https://www.nist.gov/itl/applied-cybersecurity/nice/about>.
  - [129] National Institute of Standards and Technology (NIST). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Accessed July 31, 2017.

- <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>.
- [130] National Institute of Standards and Technology (NIST). Testimony of Charles H Romine, Ph.D. Strengthening U.S. Cybersecurity Capabilities. 2017. <https://www.nist.gov/speech-testimony/strengthening-us-cybersecurity-capabilities>.
  - [131] National Institute of Standards and Technology (NIST). Notice, Request for Information—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development. ” Federal Register. July 12, 2017. <https://www.federalregister.gov/documents/2017/07/12/2017-14553/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure-workforce>.
  - [132] National Science and Technology Council. Networking and Information Technology Research and Development. Federal Cybersecurity Research and Development Strategic Plan. February 2016. [https://www.nitrd.gov/cybersecurity/publications/2016\\_Federal\\_Cybersecurity\\_Research\\_and\\_Development\\_Strategic\\_Plan.pdf](https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf)
  - [133] National Security Agency (NSA). Frequently Asked Questions. Accessed July 18, 2017. <https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml>.
  - [134] National Security Agency (NSA). Mission and Strategy. Accessed July 18, 2017. <https://www.nsa.gov/about/mission-strategy/>.
  - [135] National Security Telecommunications Advisory Committee (NSTAC). Cybersecurity Collaboration Report. 2009. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20CCTF%20Report.pdf>.
  - [136] National Security Telecommunications Advisory Committee (NSTAC). Industrial Internet Scoping Report. 2014. [https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf).
  - [137] National Security Telecommunications Advisory Committee (NSTAC). 2009-2010 NSTAC Issue Review. 2010. [https://www.dhs.gov/sites/default/files/publications/2009%20-%202010%20Issue%20Review%20%28FINAL%29\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/2009%20-%202010%20Issue%20Review%20%28FINAL%29_0.pdf).
  - [138] National Security Telecommunications Advisory Committee (NSTAC). NSTAC Report to the President on Communications Resiliency. 2011. <https://www.dhs.gov/sites/default/files/publications/NSTAC-Report-to-the-President-on-Communications-Resiliency-2011-04-19.pdf>.
  - [139] NIAC Pre-Decisional 43.
  - [140] National Security Telecommunications Advisory Committee (NSTAC). NSTAC Report to the President on Information and Communications Technology Mobilization. 2014. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf>.
  - [141] National Security Telecommunications Advisory Committee (NSTAC). NSTAC Report to the President on the Internet of Things. 2014. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf>.



- [142] National Security Telecommunications Advisory Committee (NSTAC). Telecommunications and Electric Power Interdependency Task Force (TEPITF). 2006. <https://transition.fcc.gov/pshs/docs/advisory/hkip/GSpeakers060418/ACT1070.pdf>.
- [143] North American Electric Reliability Corporation (NERC). Grid Security Exercise (GridEx II) After-Action Report. March 2014. [http://www.nerc.com/pa/CI/CIPO\\_utreach/GridEX/GridEx%20II%20Public%20Report.pdf](http://www.nerc.com/pa/CI/CIPO_utreach/GridEX/GridEx%20II%20Public%20Report.pdf).
- [144] North American Electric Reliability Corporation (NERC). Grid Security Exercise GridEx III Report. March 2016. <http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- [145] Office of the Director of National Intelligence (ODNI). Mission, Vision, & Goals. Accessed July 24, 2017. <https://www.odni.gov/index.php/who-we-are/mission-vision>.
- [146] Office of the Director of National Intelligence (ODNI). What We Do. Accessed July 24, 2017. <https://www.odni.gov/index.php/what-we-do>.
- [147] Office of Electricity Delivery & Energy Reliability (OE). Energy Sector Cybersecurity Framework Implementation Guidance. January 2015. [https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance\\_FINAL\\_01-05-15.pdf](https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf).
- [148] Office of Personnel Management (OPM). CyberCorps: Scholarship for Service, Students: Frequently Asked Questions. Accessed July 31, 2017. <https://www.sfs.opm.gov/StudFAQ.aspx#num8>.
- [149] Paganini, Pierluigi. Symantec speculates Shamoon 2 attacks aided by Greenbug hackers, Security Affairs, January 24, 2017. <http://securityaffairs.co/wordpress/55634/cyber-crime/shamoon-2-greenbug.html>.
- [150] Pagliery, Jose. Hackers destroy computers at Saudi aviation agency. CNN, December 2, 2016. <http://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/?iid=EL>.
- [151] Pritzker, Penny. U.S. Secretary of Commerce Penny Pritzker Delivers Key Note Address at U.S. Change of Commerce's Cybersecurity Summit. Written remarks, September 27, 2016. <https://www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us>.
- [152] PwC. Industry findings: Telecommunications. Excerpt from the Global State of Information Security Survey. Accessed July 19, 2017. <https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/telecommunications-industry.html>.
- [153] Sabillon, Regner, Victor Cavaller, and Jeimy Cano. National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering, No. 5. 5:67-81. May 2016. <http://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf>.
- [154] Security Scorecard. 2016 Financial Industry Cybersecurity Report. August 2016. [https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard\\_2016\\_Financial\\_Report.pdf](https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf).
- [155] Siboni, Gabi and Ofer Assaf. Guidelines for a National Cyber Strategy. The Institute for

- National Security Studies. March 2016. <http://www.inss.org.il/publication/guidelines-for-a-national-cyber-strategy/>.
- [156] Swartz, Scott D. and Michael J. Assante. Industrial Control System Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites. SANS Institute. January 2014. <https://www.sans.org/reading-room/whitepapers/ICS/securing-industrial-control-systems-2017-37860>.
- [157] Thomas, Will. Congress Passes National Defense Authorization Act. FYI: Science Policy News from AIP, American Institute of Physics, December 9, 2016. <https://www.aip.org/fyi/2016/congress-passes-national-defense-authorization-act>.
- [158] Trump for America. President-Elect Trump Announces Former Mayor Rudolph Giuliani to Lend Expertise in Cyber Security Efforts. GreatAgain Website. Accessed January 17, 2017. <https://greatagain.gov/giuliani-681188f84cb5#.6ka6242fx>.
- [159] NIAC Pre-Decisional 44.
- [160] United States Computer Emergency Readiness Team (US-CERT). “Alert (TA17-163A) CrashOverride Malware.” Accessed July 19, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- [161] The Honorable James R. Clapper, Director of National Intelligence, the Honorable Marcel Lettre, Undersecretary of Defense for Intelligence, and Admiral Michael S. Rogers, USN Commander, U.S. Cyber Command Director, National Security Agency. Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States. January 5, 2017. [https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers\\_01-05-16.pdf](https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf).
- [162] U.S. Department of Defense, U.S. Cyber Command. Beyond the Build: Delivering Outcomes through Cyberspace. June 3, 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf).
- [163] U.S. Department of Energy (DOE). Transforming the Nation’s Electricity System: The Second Installment of the Quadrennial Energy Review. January 2017. Accessed July 18, 2017. <https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment>.
- [164] U.S. Department of Energy (DOE). Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. June 2016. <https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats>.
- [165] U.S. Department of Homeland Security (DHS). Cyber Storm V: After Action Report. July 2016. [https://www.dhs.gov/sites/default/files/publications/CyberStormV\\_AfterActionReport\\_2016vFinal-%20508%20Compliant%20v2.pdf](https://www.dhs.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf).
- [166] U.S. Department of Homeland Security (DHS). Cyber Storm III Final Report. July 2011. <https://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf>.
- [167] U.S. Department of Homeland Security (DHS). Emergency Services Sector-Specific Plan. 2015. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-emergency-services-2015-508.p>

df.

- [168] U.S. Department of Homeland Security (DHS). Energy Sector-Specific Plan. 2015. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf>.
- [169] U.S. Department of Homeland Security (DHS). Financial Services Sector. Last updated July 6, 2017. <https://www.dhs.gov/financial-services-sector>.
- [170] U.S. Department of Homeland Security (DHS). Financial Services Sector-Specific Plan. 2015. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf>.
- [171] U.S. Department of Homeland Security (DHS). Industrial Control Systems Cyber Emergency Response Team. Accessed July 19, 2017. [https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT\\_FactSheet\\_ICS-CERT\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf).
- [172] U.S. Department of Homeland Security (DHS). Healthcare and Public Health Sector-Specific Plan. 2016. Accessed July 20, 2017. <https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf>.
- [173] U.S. Department of Homeland Security (DHS). Informing Cyber Storm V: Lessons Learned from Cyber Storm IV. 2015. <https://www.dhs.gov/cyber-storm-v>.
- [174] U.S. Department of Homeland Security (DHS). National Cybersecurity and Communications Integration Center. Last updated June 22, 2017. <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>.
- [175] U.S. Department of Homeland Security (DHS). National Cyber Incident Response Plan. December 2016. Accessed July 18, 2017. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- [176] U.S. Department of Homeland Security (DHS). NCCIC/ICS-CERT Year in Review FY 2015. Accessed July 17, 2017. [https://ics-cert.us-cert.gov/sites/default/files/Annual\\_Reports/Year\\_in\\_Review\\_FY2015\\_Final\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf).
- [177] U.S. Department of Homeland Security (DHS). National Protection and Programs Directorate Cybersecurity Legal Authorities Overview. Accessed July 31, 2017.
- [178] U.S. Department of Homeland Security (DHS). U.S. Government Support for Critical Infrastructure Cybersecurity Risk Management Authorities and Capabilities Matrix. Accessed July 31, 2017.
- [179] U.S. Government Accountability Office (GAO). Cybersecurity: Actions Needed to Strengthen U.S. Capabilities. February 14, 2017. <https://www.gao.gov/assets/690/682757.pdf>.
- [180] NIAC Pre-Decisional 45.
- [181] U.S. Government Accountability Office (GAO). Federal Information Security: Actions Needed to Address Challenges. September 19, 2016. <http://www.gao.gov/assets/680/679877.pdf>.
- [182] The White House. Executive Order--Commission on Enhancing National Cybersecurity. February 9, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity>.
- [183] The White House. Executive Order—Improving Critical Infrastructure Cybersecurity.

- February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
- [184] The White House. Executive Order—Promoting Private Sector Cybersecurity Information Sharing. February 13, 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- [185] The White House. Executive Order—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 11, 2017. <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.
- [186] The White House. Fact Sheet: Cybersecurity National Action Plan. February 9, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.
- [187] The White House. Fact Sheet: Cyber Threat Intelligence Integration Center. February 25, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center>.
- [188] The White House. Presidential Policy Directive – Critical Infrastructure Security and Resilience. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- [189] The White House. Statement by the President on Signing the National Defense Authorization Act for Fiscal Year 2017. Press release, December 23, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/12/23/statement-president-signing-national-defense-authorization-act-fiscal>.
- [190] The White House. Strengthening the Federal Cybersecurity Workforce. Press release, July 12, 2016. <https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce>.

---

# 附录 I 美国 CSIS 对特朗普政府的网络安全建议（摘要）

从意识到行动——第 45 任总统网络安全议程  
美国战略与国际研究中心（CSIS）网络政策工作组<sup>①</sup>

2017 年 1 月

---

---

<sup>①</sup> CSIS 有为美国总统在上任之初提交网络安全政策建议的传统。其为第 44 任美国总统（奥巴马）提交的网络安全政策建议对奥巴马政府产生了重要影响，CSIS 也因此成为美国政府所倚重的知名网络安全智库。——译者注

本报告为下一届政府得以建立更好的网络安全政策、资源和组织而提出了可操作的方案。国家改善网络安全的目标仍然是始终如一的，即建立一个安全稳定的数字环境，以支持经济的持续增长，同时还要保护个人自由和国家安全。对该目标的实施要求也是始终如一的，即以白宫为中心指导和顶层领导，建立并实施一套全面、协调的网络安全方案。2008 年以来，政府已经做了很多工作，但下届政府仍应在原有基础上加强和改进。第 45 任总统应：

- 基于与志同道合国家建立的伙伴关系，制定新的国际战略，通过发展不止于军事行动的全面响应和反制能力，以提高对攻击者的威慑力。
- 持续提供内阁级的支持，以建立打击僵尸网络和复杂的金融犯罪活动的国际合作机制，认真、努力地减少网络犯罪。其中，必须惩罚那些不愿意以合作方式减少和控制网络犯罪的国家。
- 使关键基础设施和服务为应对攻击做好准备，提升其“安全健康”水平。新政府应采取可能的激励措施。但如果激励措施不管用，就要随时考虑进行监管。要更多地使用托管服务，使政府机构更加安全。
- 明确在哪些地方需要联邦投入资源，例如在研究和人才队伍建设问题上，虽然多数这样的工作留给了私营部门来完成。我们不需要网络版的“曼哈顿计划”。
- 减少白宫的官僚主义，在审计总署（GAO）创建一个专门的办公室，以加强联邦政府对网络安全的监督，同时明确国防部和其他机构的角色。一个强大的国土安全部对网络安全而言至关重要，新政府必须强化国土安全部，否则就将网络安全职能转移到别的部门。

下届政府应遵循两个指导原则：要使国外攻击者遭受惩罚，对国内行为者予以激励。对网络犯罪、间谍以及网络攻击行为追责，这是降低网络安全风险最有效的方式（特别是与志同道合的国家合作实施）。风险是无法被完全消除的，重要的关键基础设施要采用高标准，同时还要通过游说、调整税收政策、监管和投资措施来激励普通大众中的在线行为者来改进其行为，从而实现更好的安全状态。这些工作还需要一些进一步的资源，但资源方面的限制并不是阻碍网络安全水平得以提升的主要障碍。无论以前还是现在，真正的障碍是组织的无序、政府角色的混乱以及缺少足够的意愿。

华盛顿和硅谷的团队编写了共 14 份工作文件和 220 份对新政府的具体建议。这些建议概述如下：

## 1. 政策

网络安全的环境已经发生了变化，美国在该方面的自信心和影响力受到了世界上多个国家的挑战。俄罗斯将网络视为一种国家力量工具，这一做法令人感到震惊和担忧。大量事件，如朝鲜、伊朗分别对索尼和金沙赌场的入侵，以及中国黑客对人事管理局（OPM）的入侵<sup>①</sup>，反映了各国利用网络工具对我国实施攻击的意愿在逐渐增强。国际安全形势的不断恶化，意味着

---

① 针对美国对中国网络攻击的无端指责，我国外交部等部门已经表明严正立场，对美指责予以驳斥，并重申反对一切形式的网络攻击。为了体现原文，本处没有删改，但不表示译者支持或认同 CSIS 的表述。——译者注

下届政府将面临形势更加严峻的网络犯罪和间谍活动，同时也面临着个人信息和企业数据遭到威胁、以政治施压为目的的网络恶意活动增多，以及关键基础设施可能会遭受破坏或攻击的风险。面对如此巨大的风险，美国需要采取国际和国内行动进行响应。

### 国际战略

很显然，这些年来，网络安全的全球化方案一直受到限制。我们与专制国家只能达成关于网络规则的有限协议。这些专制国家更在意保护主权以及减少信息技术带来的政治和军事上的威胁，这就限制了与其达成的网络协议的覆盖范围，无法实现降低风险的目的。相较之下，下届总统将有机会与志同道合的民主国家达成协议，建立起一个强健的国际网络安全架构。任何考虑都要看一看，现在是不是采取更正式方法的时候，包括建立更好的制度或机制来维护网络空间的安全和稳定。

和一些国家打交道的经验告诉我们，可以让对手的行为发生改变，风险环境可以被美国的行动所重塑。上两届美国政府一直没有找到有效的网络威慑政策，问题可能出在试图使用军事力量。最有效的威慑方法不是军事介入，而是威胁进行制裁或起诉，这是一种不需要武力的报复行为。“如果把威慑看作一个梯子，那么要把威慑力量分布到这个梯子的每根横木上”。要有适宜的非军事应对手段，并且要让对手知道这些手段，这是有益的做法。但目前对外的宣传政策不仅冗长而且混乱，很不清晰，削弱了威慑的有效性，必须另起炉灶。值得注意的是，即使有着更为明确的威慑政策，包括更清晰的宣传政策和更广泛的应对方案，某些对手也不会受到阻止。这表明，我们需要在提升网络安全防御能力上做更多的工作，但这件事也会使我们与一些国家之间的关系出现更大的问题。

### 更加决断地打击网络犯罪

网络犯罪问题已经非常广泛，其跨国性使国际合作成为唯一有效的应对方式。但有些国家甚至根本不考虑合作。下届政府需要制定新的惩罚方式，现有的惩罚方法已经过时了。《布达佩斯网络犯罪公约》也因为那些试图将网络犯罪作为政治工具及新型力量的国家的反对而陷入僵局，它们拒绝签署这个条约，不愿意进行协商。我们需要打破《布达佩斯网络犯罪公约》的僵局，提出一种新的协商方式，以保护该公约的利益，并吸引巴西、印度和其他国家的加入。有人认为公约的重新开放会降低其公信力，但其他可能的替代性方案却迟迟未见出台。

### 保护全球数据流

我们思考网络安全的方式之一是，我们正在为安全的数字经济建立一个体系结构，而数据流是这个经济里的“货币”。下届政府需要与其他国家合作，以确保数据自由、安全流动。这需要对国际网络安全、隐私和数字贸易的规则（或许是体制）进行探讨。还包括与志同道合国家达成协议，这些协议要建立在隐私和公民自由基线标准的基础之上。其中，一项重要的工作是改进《法律互助条约》进程。

### “基线”网络安全、关键基础设施与 NIST 框架

所有的组织都有义务去加强网络安全建设，这不仅是保护其业务经营和客户数据的安全，也有利于整个互联数字社会本身。网络安全方面的工作进展是，已要求各类组织改进基线网络安全，采取简化措施和最佳实践，因为这些措施和最佳实践在降低风险方面有着非常显著的效

果。其中的关键是实施更好的网络安全治理、提升网络“安全健康”水平、采用更快的技术“更新”周期、改善身份鉴别方法（不能只用口令对重要数据进行保护），以及鼓励大家对数据泄露事件进行披露。

2013 年 2 月的总统行政令对关键基础设施保护采取了一种自愿的、体现各部门特色的方案。该方法基于美国国家标准与技术研究院（NIST）的“网络安全框架”，要求每个监管机构都对自己对口的关键基础设施部门负责。尽管其不完美，但网络安全政治学意味着这起码是当下最优的。下届总统应推动或在必要时强制执行该框架。可以研究一下如何衡量各机构的采纳情况及其有效性。NIST 应与私营部门合作，成立工作组研究这些指标。

### **数据保护、隐私和网络安全**

保护国家的网络资产也包括保护敏感的个人信息。鉴于网络空间遍布脆弱性和威胁，那些收集和留存数据的人对网络安全负有更大的责任。此外，随着全球日益关注数据保护，美国需要明确，其准备采取何种措施保护数据。下届政府应将数据保护纳入更全局的网络安全方法之中，并坚持“数据属于用户”的原则。总统要求联邦贸易委员会（FTC）建立数据保护处，这是一项可以推进的工作。还有一项可以推进的工作是制定关于国家数据泄露的立法。要先制定一部标准，把数据保护焦点放到专门的、已经想明白的领域，并为其他的重大改革提供立法工具。

### **提高网络事件的透明度**

2012 年之后，大部分网络安全讨论都专注于信息共享。2015 年《网络安全法》的通过结束了这一讨论，但仍感觉需在两个方面做更多的工作。首先，是打破涉密的网络威胁和攻击信息如何公布的僵局，其实很多这类信息在公布时并不会对情报源和情报方法带来风险。

其次，一旦公布细节，就需要为网络攻击的受害者提供可靠的保护。尽管 2015 年的立法已经考虑了这一问题，但保护范围还需扩大。那些被黑过的人往往不愿分享信息，因为如果将被黑经历广而告之，可能会损害其收入、股票价格和声誉。因此，有效的事件报告发布方案需要实施匿名和责任保护。我们可以学习国家交通安全委员会在调查空难或者联邦航空局在航空安全报告系统中的实际作法，即全面禁止将所提交的信息用于执法目的。此项新工作可以由国土安全部或网络威胁信息整合中心负责。

### **为物联网（IoT）做好准备**

物联网的普及意味着硬件和软件将不可避免地出现故障，遭到黑客攻击的可能性也将不可避免地增加。因此物联网产品必须负起安全责任来。如果联邦政府不干预，那么相关技术标准将呈现分散式发展的趋势，潜在后果是不利的。我们向下届政府建议：（1）NIST 要与消费者和商业组织合作，共同制定物联网相关安全标准和原则；（2）安全方法要能反映各关键基础设施部门的特色；（3）要使用联邦采购标准来推动变革，保护政府职能的运转。可以借鉴国家公路交通安全管理局的碰撞试验，建立公开的物联网安全评级制度。

### **加密政策**

对加密技术的广泛使用可以提升整体网络的安全性，但具体加密方式和实现方法会对国家安全产生重大影响。美国制定的任何加密政策和法律框架都必须考虑到全球环境和美国的国际网络安全战略。美国政策应支持使用强加密方案，但同时应明确指出，在何种条件下应协助执



法机构以合法方式访问数据。最终，加密政策需要对相关的风险做出决策。无限制地使用加密技术，会增加犯罪和恐怖主义的风险，但相对于限制使用加密技术而言，各国会发现，上述风险是可以接受的。我们的朋友圈中，没有任何国家认为现有风险已经大到需要对加密进行新的限制。

## 2. 组织

奥巴马政府为国土安全部赋予了网络安全责任。在过去 4 年内，网络安全虽有所改善，但一些专家仍认为，同国家安全局（NSA）相比，国土安全部能力还是不足，他们更希望国防部来负责网络安全。但私营部门对此却不支持，它们更希望由一个民事部门来负责。如果坚持由国土安全部负责，就必须对其网络使命进行改革。目前的最佳解决方案是剥离国家保护与计划处的无关职能，并将其提升成为国土安全部的一个局级单位（类似于海岸警卫队或特勤处）。该新机构应回避情报或执法任务，而是将工作重心放在缓解网络安全问题上（帮助企业为应对网络攻击做好准备，以及从网络攻击中恢复）。过去 10 年，国土安全部一直领导着此类事务。如果这一改革无法顺利完成或运转无效，那干脆就把网络安全职能从国土安全部剔除好了。

新政府上任之后应尽快发布一份对各机构角色和职责的清晰声明，以尽量减少机构间的争端。在这份声明中，应当定义国防部如何在网络安全事件处置中支持国土安全部，国土安全应如何支持联邦调查局的调查，以及为了应对攻击，“接力棒”应何时从国土安全部移交给国防部。要制定相关政策和条例，说明国防部在危机或紧急情况下应如何采取行动，特别是涉及外国网络行为体的时候。国防部不应承担监管职能，也不应承担和平时期的职能。上届政府在白宫内设立了很多职位，如首席技术官、首席信息安全官等，这些职位都缺乏权限和资源，可以取消。同样，科技政策办公室（OSTP）在网络安全方面的角色也没什么用。

联邦机构的网络安全也是个问题。解决方案可以是采用托管服务，但审计总署（GAO）也应获得授权，便于对联邦网络安全进行独立的国会审查，包括渗透性测试等。

## 3. 资源

### 减少脆弱性

美国在企业和机构层已投入了数十亿美金研发不同的网络安全技术，以保护我们的网络。然而这是一种被动、碎片化的方法，攻击者可以逃避。美国需要有更主动的方法，对“漏洞奖励”和“零日漏洞项目”增加投资和关注，使发现脆弱性的研究人员获得奖励。这些工作将有很大的回报，美国政府应予大力支持，并进一步强调互联网基础设施安全保护工作和开源软件的广泛应用。重要一点是，要阐明这些方案的合法性，为研究人员提供安全避风港，使安全研究能成为一个产业，在脆弱性研究行为规范指导下得以发展壮大。

### 提高对共享服务和云服务的使用

大部分联邦机构都不涉及网络安全方面的业务。但网络安全的确需要得到足够的保护，这使得各机构不得不心生旁骛。而网络安全专家的数量更少，这进一步加剧了问题的复杂度。美国政府需要反思，为了实现更好的网络安全，应如何去获取和管理信息技术。应当转向托管服

务模式，将电子邮件、数据存储和网络安全承包给小机构。管理和预算办公室（OMB）同总务管理局（GSA）正在实施一个将网络安全纳入 IT 采购及项目的活动，托管模式是这项工作的一部分。与自行管理的一般 IT 架构相比，云服务有着显著的安全优势，其成本更低、效率更高。将基础性的安全功能外包后，更有利于实施威胁共享，各类组织可以将其资源集中于处理那些非常关键或罕见的网络风险，以防止出现最严重的后果。

### **扩大网络安全人才队伍**

由于需求日益增长，招聘训练有素的网络安全人才正变得愈加困难。为了解决这一问题，下届政府应积极推行网络安全教育和人才队伍计划，如建立经认可的培训与教育制度，对网络安全角色及网络安全从业者的具备的专业技能进行分类，以及发展一批可靠的专业资质认证机构。

### **着眼未来**

当前网络安全政策已经非常被动，变得碎片化，且少有不是这样的。为此，应制定新的战略。但历史经验却令人沮丧，很多战略充斥着陈词滥调，而且在网络安全问题上，它们无非是列出了一些详细的药方，根本没有上升到战略层，往往很快就过时了。

20 年来的经验表明，单纯把重点放在强化网络本身是不够的。企业 and 国家必须充分理解其在网络空间应如何行动，并且明确这些行动规则。没有哪个问题是不能克服的，但所有问题的解决都离不开高层的持续关注以及脚踏实地的努力。

网络空间已经成为核心的全球性基础设施，其重要性只会不断提高。但它是不安全的，我们面临的风险完全没有必要这么严重。我们的对手仍保有优势。只要我们有意愿，我们就可以改变这种局面，尽管没那么快，也没那么容易。但为了美国及盟国的安全，这都是必要的。

---

## 附录Ⅱ 主要缩略语

---

AACC	American Association of Community Colleges	美国社区学院协会
AAR	Association of American Railroads	美国铁路协会
AASCU	American Association of State Colleges and Universities	美国州立学院和大学协会
AAU	Association of American Universities	美国大学协会
AAUPSAFEC	American Association of University Professors Statement on Academic Freedom in Electronic Communications	美国大学教授声援电子通信学术自由协会
ABA	American Bankers Association	美国银行家协会
ACC	American Chemistry Council	美国化学联合会
ACE	American Council on Education	美国教育联合会
ACERT	Army Computer Emergency Response Team	陆军应急响应小组
ACTD	Advanced Concept Technology Demonstration	先期概念技术演示
AFWIC	Air Force Warfare Information Center	空军作战信息中心
AGA	American Gas Association	美国天然气协会
AICPA	American Institute of Certified Public Accountants	美国注册公共会计师协会
AIDE	Automated Intrusion Detection Environment	自动化入侵检测环境
AISU	Analysis and Information Sharing Unit	分析和信息共享处
ANSI	America National Standards Institute	美国国家标准学会
ANSIR	Awareness of National Security Issues and Response System	国家安全意识发布和响应系统
ARL	Association of Research Libraries	科研图书馆协会
ASDC <sup>3</sup> I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence	国防部指挥、控制、通信和情报助理部长
ATF	Bureau of Alcohol, Tobacco and Firearms	烟草、酒精和枪支管理局
AWWA	American Water Works Association	美国水工业协会
AWWARF	AWWA Research Foundation	美国水工业协会研究基金会
A&I	Assurance and Integration	保障和集成
B&F	Banking and Finance	银行与金融
BCP	Business Continuity Planning	业务连续性计划
BGP	Border Gateway Protocol	边界网关协议
BITS	Banking Industry Technology Secretariat	银行业技术秘书处
BPC	Business Continuity Planning Committee	业务连续性计划委员会

CA	Certificate Authority	认证中心
CDC	Centers for Disease Control and Prevention	疾病控制和预防中心
CEO	Chief Executive Officer	首席执行官
CERT	Computer Emergency Response Team	计算机应急响应小组
CERT/CC	Computer Emergency Response Team/Coordination Center	计算机应急响应小组/协调中心
CEST	Cyber-Emergency Support Team	网络应急支持组
CFO	Chief Financial Officer	首席财政官
CIA	Central Intelligence Agency	中央情报局
CIAC	Computer Incident Advisory Capability	计算机事件咨询功能中心
CIAO	(1) Critical Infrastructure Assurance Office (2) Chief Infrastructure Assurance Officer	(1) 关键基础设施保障办公室 (2) 首席基础设施保障官
CICG	Critical Infrastructure Coordination Group	关键基础设施协调组
CIDX	Chemical Industry Data eXchange	化学工业数据交流组织
CIKR	Critical Infrastructure and Key Resource	关键基础设施与重要资源
CIO	Chief Information Officer	首席信息官
CIP	Critical Infrastructure Protection	关键基础设施保护
CIP IWG	Critical Infrastructure Protection Interagency Working Group	关键基础设施保护跨机构协调组
CIPP	Defense Critical Infrastructure Protection Program	国防部关键基础设施保护项目
CIPIS	Critical Infrastructure Protection Integration Staff	关键基础设施保护综合参谋处
CIPRDI	Critical Infrastructure Protection Research and Development Initiative	关键基础设施保护研发活动
CIRT	Computer Incident Response Team	计算机事件响应小组
CISO	Chief Information Security Officer	首席信息安全官
CISSP	Certification for the Information Systems Security Profession	信息系统安全专家认证
CITE	Center for Information Technology Excellence	信息技术优秀中心
CIWG	Critical Infrastructure Working Group	关键基础设施工作组
CMF	Cyber Mission Force	网络任务部队
CMP	Coordinated Management Process	协调管理过程
CNA	Computer Network Attack	计算机网络攻击
CNAP	Cybersecurity National Action Plan	国家网络安全行动计划

CNCI	Comprehensive National Cybersecurity Initiative	综合性国家网络安全计划
CNSS	Committee on National Security Systems	国家安全系统委员会
COBIT	Control Objectives Information and Related Technologies	信息及相关技术控制目标
COMAFFOR	Commander, Air Force Forces	空军指挥官
COMARFOR	Commander, Army Forces	陆军指挥官
COMMARFOR	Commander, Marine Forces	潜艇部队指挥官
COMNAVFOR	Commander, Navy Forces	海军指挥官
COO	Chief Operating Officers	首席运营官
COTS	Commercial Off-the-Shelf	商业现货
CPDF	Central Personnel Data File	中央人事数据档案
CREN	Consortium for Research and Education Networking	科研和教育网络协会
CRG	Cyber Response Group	网络响应小组
CSF	Cyber Security Framework	网络安全框架
CRL	Certificate Revocation List	证书注销列表
CSI	Computer Security Institute	计算机安全学会
CSIRC	Computer Security Incidence Response Capability	计算机安全事件响应功能中心
CSTB	Computer Science and Telecommunications Board	计算机科学和电信委员会
CTIA	Cellular Telecommunications and Internet Association	移动通信与 Internet 协会
CTIIC	Cyber Threat Intelligence Integration Center	网络威胁情报整合中心
CWIN	Cyber Warning and Information Network	网络预警和信息网
DARPA	Defense Advanced Research Projects Agency	国防部高级研究计划局
DASD	Deputy Assistant Secretary of Defense	国防部常务助理部长
DCS	Digital Control System	数字控制系统
DDoS	Distributed Denial of Service Attack	分布式拒绝服务攻击
DERA	Defense Evaluation and Research Agency	国防部评估和研究局
DFAS	Defense Finance and Accounting Service	国防部金融和会计业务局
DHRA	Defense Human Resources Agency	国防部人力资源局
DHS	Department of Homeland Security	国土安全部
DI	Defense Infrastructure	国防基础设施
DIA	Defense Intelligence Agency	国防情报局

DIAP	Defense-wide Information Assurance Program	国防信息保障项目
DII	Defense Information Infrastructure	国防信息基础设施
DIO	Defensive Information Operations	防御性信息作战
DISA	Defense Information Systems Agency	国防信息系统局
DLA	Defense Logistics Agency	国防部后勤局
DOC	Department of Commerce	商务部
DoD	Department of Defense	国防部
DoDD	Department of Defense Directive	国防部令
DoDIN	DoD Information Network	国防部信息网
DOE	Department of Energy	能源部
DOI	Department of the Interior	内务部
DOJ	Department of Justice	司法部
DOL	Department of Labor	劳工部
DOS	Department of State	国务院
DoS	Denial-of-Service attacks	拒绝服务攻击
DOT	Department of Transportation	交通部
DSL	Digital Subscriber Line	数字用户线路
DVA	Department of Veterans Affairs	退伍军人事务部
ECC	Emergency Command Center	应急指挥中心
EEI	Edison Electric Institute	爱迪生电力研究所
EO	Executive Order	行政令
EOP	Executive Office of the President	总统行政办公室
EPA	Environmental Protection Agency	环境保护局
ECPA	Electronic Communications Privacy Act	电子通信隐私法
ELES	Emergency Law Enforcement Services Sector	应急执法服务部门
ERP	Federal Response Plan	联邦响应计划
ERT	Expert Review Team	专家评审组
EPRI	Electric Power Research Institute	电力研究院
ESF	Emergency Support Function	应急支持功能
EU	European Union	欧盟
FAA	Federal Aviation Administration	联邦航空管理局
FBI	Federal Bureau of Investigation	联邦调查局
FBIIC	Financial and Banking Information Infrastructure Committee (of the PCIPB)	(PCIPB 的) 金融和银行信息基础设施委员会

FCC	Federal Communications Commission	联邦通信委员会
FCS	Federal Computer Services	联邦计算机服务
FedCIRC	Federal Computer Incident Response Capability	联邦计算机事件响应功能中心
FEIEC	Federal Financial Institutions Examination Council	联邦金融机构的检查委员会
FEIT	Functional Evaluation and Integration Team	功能评估和集成中心
FEMA	Federal Emergency Management Agency	联邦应急管理局
FFRDC	Federally Funded Research and Development Center	联邦基金研究和开发中心
FERC	Federal Energy Regulatory Commission	联邦能源管制委员会
FERPA	Family Educational Rights and Privacy Act	家庭教育权和隐私权法
FIDNet	Federal Intrusion Detection Network	联邦入侵检测网
FIRST	Forum of Incident Response and Security Teams	事件响应和安全小组论坛
FISSEA	Federal Information Systems Security Educators' Association	联邦信息系统安全教育者协会
FMS	Financial Management Services	金融管理部
FOC	Full Operating Capability	全面运行能力
FOIA	Freedom of Information Act	信息自由法
FPKISC	Federal PKI Steering Committee	联邦公钥基础设施指导委员会
FRB	Federal Reserve Board	联邦储备委员会
FS/ISAC	Financial Service / Information Sharing Analysis Center	金融服务共享和分析中心
FTC	Federal Trade Commission	联邦贸易委员会
FY	Fiscal Year	财政年度
GAO	General Accounting Office	审计总署
GCC	Government Coordinating Council	政府协调委员会
GDP	Gross Domestic Product	国内生产总值
GETS	Government Emergency Telecommunications Service	政府应急电信服务
GII	Global Information Infrastructure	全球信息基础设施
GIS	Geographic Information System	地理信息系统
GISRA	Government Information Security Reform Act of 2000	2000 年政府信息安全改革法
GNOSC	Global Network Operations and Security Center	全球网络作战和安全中心



GOTS	Government Off-the-Shelf	政府现货
GPRA	Government Performance and Results Act	政府绩效和结果法
GPS	Global Positioning System	全球定位系统
GRI	Gas Research Institute	天然气研究院
GSA	General Services Administration	总务管理局
HEITA	Higher Education Information Technology Alliance	高等教育信息技术联盟
HHS	Department of Health and Human Services	健康和公众服务部
HIPAA	Health Insurance Portability and Accountability Act	健康保险可携带性和责任法
HSI	Homeland Security Investigations	国土安全调查局
HUD	Department of Housing and Urban Development	住房和城市发展部
I <sup>3</sup> P	Institute for Information Infrastructure Protection	信息基础设施保护学会
I&C	Information and Communications	信息与通信
I&W	Indications and Warnings	迹象发现和预警
IA	Information Assurance	信息保障
IAP	Information Assurance Program	信息保障项目
IAVA	Information Assurance Vulnerability Alert	信息保障脆弱性报警
IC	Intelligence Community	情报共同体
ICANN	Internet Corporation for Assigned Names and Numbers	Internet 域名与数字地址分配机构
ICBA	Independent Community Bankers of America	美国独立社区银行家协会
ICC	Information Coordination Center	信息协调中心
ICE	Immigration and Customs Enforcement	移民和海关执法局
ICI-IPC	Infrastructure Interagency Policy Committee	基础设施跨部门政策委员会
ICS	Incident Command System	事件指挥系统
IDS	Intrusion Detection System	入侵检测系统
IEEE	Institute of Electrical and Electronics Engineers	电子电气工程师学会
IETF	Internet Engineering Task Force	Internet 工程任务组
IFCC	The Internet Fraud Complaint Center	Internet 欺诈诉讼中心
IG	Inspector General	总检查长
IIA	Institution of Internal Auditors	内部审计师学会
IIPO	Information Integration Program Office	信息整合项目办公室
IIWG	International Interagency Working Group	国际跨机构工作组

IHE	Institution of Higher Education	高等教育学会
INFOSEC	Information Security	信息安全
IOC	Initial Operating Capability	初等运行能力
IP	Internet Protocol	Internet 协议
IRM	Information Resource Management	信息资源管理
ISAC	Information Sharing and Analysis Center	信息共享和分析中心
ISACA	Information Systems Audit and Control Association	信息系统审计与控制协会
ISAO	Information Sharing and Analysis Organization	信息共享和分析组织
ISO	International Standards Organization	国际标准化组织
ISP	Internet Service Provider	Internet 服务提供商
ISSO	Information Systems Security Officers	信息系统安全官
ISSS	Information Systems Security Strategy	信息系统安全战略
IT	Information Technology	信息技术
ITAA	Information Technology Association of America	美国信息技术协会
ITMRA	Information Technology Management Reform Act	IT 管理改革法
ITO	Information Technology Office	信息技术办公室
ITU	International Telecommunications Union	国际电信联盟
IWG	Interagency Working Group	跨机构工作组
JIACTF	Joint Interagency Cyber Task Force	跨部门联合网络任务组
JTF-CND	Joint Task Force-Computer Network Defense	计算机网络防护联合特别任务中心
KAI	Key Asset Initiative	关键资产行动
LAN	Local Area Networks	局域网
LEA	Law Enforcement Agencies	执法机构
MISPC	Minimum Interoperability Specification for PKI Components	PKI 组件最小互操作规范
NACD	National Association of Corporate Directors	全美公司董事联合会
NACUBO	National Association of College and University Business Officers	学院和大学商务官员全国协会
NAICU	National Association of Independent Colleges and Universities	独立学院和大学全国协会
NASA	National Aeronautics and Space Administration	国家宇航管理局

NASCIO	National Association of State Chief Information Officers	全国州首席信息官协会
NASULGC	National Association of College and Universities and Land-Grant Colleges	州立大学和政府赠地学院全国协会
NCA	National Command Authority	国家指挥中心
NCCIC	National Cybersecurity and Communication Integration Center	国家网络安全和通信整合中心
NCIJTF	National Cyber Investigative Joint Task Force	国家网络调查联合特遣队
NCIRP	National Cyber Incident Response Plan	国家网络事件响应计划
NCS	National Communications Systems	国家通信系统委员会
NCSC	National Cyber Security Center	国家网络安全中心
NCTP	National Cybercrime Taining Partenership	国家网络犯罪防范培训联盟
NDPO	National Domestic Preparedness Office	国家国内战备办公室
NEC	National Economy Council	国家经济委员会
NERC	North American Electric Reliability Council	北美电力可靠性委员会
NETS	National Education and Technology Standards	国家教育和技术标准
NGA	National Governors' Association	全国州长协会
NGN	Next Generation Network	下一代网络
NIAC	National Infrastructure Assurance Council	国家基础设施保障委员会
NIAP	National Information Assurance Partnership	国家信息保障联盟
NIETP	National INFOSEC Education and Training Program	国家 Inforsec 教育和培训项目
NIH	National Institutes Health	全国健康学会
NII	National Information Infrastructure	国家信息基础设施
NIMS	National Incident Management System	国家事件管理体系
NIPC	National Infrastructure Protection Center	国家基础设施保护中心
NIPCIP	National Infrastructure Protection and Computer Intrusion Program	国家基础设施保护和计算机入侵项目
NIPP	National Infrastructure Protection Plan	国家基础设施保护计划
NISAC	National Infrastructure Simulation and Analysis Center	国家基础设施仿真和分析中心
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NLETS	National Law Enforcement Telecommunications System	国家执法通信系统
NMCC	National Military Command Center	国家军事指挥中心

NMCIAC	New Mexico Critical Infrastructure Assurance Council	新墨西哥州关键基础设施保障委员会
NMERI	New Mexico Engineering Research Institute	新墨西哥州工程研究院
NPC	National Plan Coordination	国家计划协调处
NPC	National Petroleum Council	国家石油委员会
NRF	National Response Framework	国家响应框架
NRIC	Network Reliability and Interoperability Council	网络可靠性和互操作性委员会
NRC	Nuclear Regulatory Commission	原子能管制委员会
NSA	National Security Agency	国家安全局
NSAA	National State Auditors Association	全国州审计师协会
NSC	National Security Council	国际安全委员会
NSD	National Security Directive	国家安全令
NS/EP	National Security/Emergency Preparedness	国家安全/应急战备
NSF	National Science Foundation	国家科学基金会
NSGIC	National State Geographic Information Council (NSGIC)	全国州地理信息委员会
NSIRC	National Security Incident Response Center	国家安全事件响应中心
NSTAC	National Security Telecommunications Advisory Council	国际安全电信咨询委员会
NSTISSC	National Security Telecommunications and Information Systems Security Committee	国际安全电信和信息系统安全委员会
NTAC	National Threat Assessment Center	国家威胁评估中心
NTIA	National Telecommunications & Information Administration	国家电信和信息管理局
NW3C	National White Collar Crime Center	国家白领犯罪中心
OASD	Office of the Assistant Secretary of Defense	国防部助理部长办公室
ODNI	Office of the Director of National Intelligence	国家情报总监办公室
OECD	Organization for Economic Cooperation and Development	经济合作与发展组织
OMB	Office of Management and Budget	管理和预算办公室
OPM	Office of Personnel Management	人事管理办公室
OSD	Office of the Secretary of Defense	国防部长办公室
OSTP	Office of Science and Technology Policy	科技政策办公室
PATRIOT	Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act	提供所需的合适工具来拦截恐怖分子法（也称爱国者法）

PCAST	President's Commission of Advisors on Science and Technology	总统科技咨询委员会
PCCIP	President's Commission on Critical Infrastructure Protection	关键基础设施保护总统委员会
PCIPB	President's Critical Infrastructure Protection Board	总统关键基础设施保护委员会
PCIE	President's Council on Integrity and Efficiency	廉政和效率总统委员会
PCIS	Partnership for Critical Infrastructure Security	关键基础设施安全合作组织
PCS	Process Control Systems	过程控制系统
PDD	Presidential Decision Directive	总统令
PITAC	President's Information Technology Advisory Council	总统信息技术资源委员会
PKI	Public Key Infrastructure	公钥基础设施
PNNI	Private Network-to-Network Interface	专用网到网接口
POC	Point-of-Contact	联络人
POTUS	President of the United States	美国总统
PPBS	Planning, Programming, and Budgeting System	计划、规划和预算系统
PSTN	Public Switched Telecommunications Network	公共交换电信网
QoS	Quality of Service	服务质量
R&D	Research and Development	研究和开发
RAL	Registered Asset List	注册资产列表
SANS	SysAdmin, Audit, Networking and Security	系统管理、审计、联网和安全 (学会)
SBA	Small Business Administration	小型商业管理局
SCADA	Supervisory Control and Data Acquisition	监督控制和数据采集
SCC	Sector Coordinating Council	部门协调理事会
SEC	Securities Exchange Commission	证券交易委员会
SECDEF	Secretary of Defense	国防部长
SFS	Scholarship For Service	服务奖学金
SIA	Securities Industry Association	证券工业协会
SLTT	State, Local, Tribal, Territorial	州、地方、部落和领地
SMI	Security Management Infrastructure	安全管理基础设施
SRO	Self-regulated Organization	自律性组织

SSA	Sector Specific Agency	(关键信息基础设施) 部门对口机构
SSE-CMM	System Security Engineering-Capability Maturity Model	系统安全工程-能力成熟度模型
ST-ISAC	Surface Transportation ISAC	地面运输-信息共享和分析中心
SWIFT	Society for Worldwide Interbank Financial Transactions	国际银行间金融交易协会
TBD	To Be Determined	待定
TCP/IP	Transport Control Protocol / Internet Protocol	传输控制协议/Internet 协议
TFI	The Fertilizer Institute	美国化学学会
TIA	Telecommunications Industry Association	电信工业协会
TIC	Trusted Internet Connection	可信互联网连接
TSP	(1) Telecommunications Service Priority (2) telecommunications service provide	(1) 电信服务优先级 (2) 电信服务提供商
TSWG	Technical Support Working Group	技术支持工作组
UCEA	University Continuing Education	大学成人教育协会
UCG	Unified Coordination Group	统一协调小组
UTC	The United Telecom Council	联合电信委员会
USDA	Department of Agriculture	美国农业部
USTA	United States Telecom Association	美国电信协会
VHS	Vital Human Services	重要民生服务
VPN	Virtual Private Network	虚拟专用网
WAAS	Wide-Area Augmentation System	广域增强系统
WAN	Wide Area Networks	广域网
WDM	Wavelength Division Multiplexing	波分复用
WLAN	Wireless Local Area Network	无线局域网
WWU	Watch and Warning Unit	观察和预警处
Y2K	Year 2000	“千年虫” 问题

# 致 谢

早在美国于 1998 年发布第 63 号总统令《对关键基础设施保护的政策》时，沈昌祥院士、赵战生教授便提议对美国网络安全战略进行持续跟踪研究，此后一直指导、支持这项工作。

中国电子信息产业集团芮晓武董事长十分关心本书的编译，给予了大量人力、物力支持。

全书主要编译者如下：第一篇（左晓栋），第二篇（左晓栋），第三篇（左晓栋），第四篇（左晓栋），第五篇（孙锐、左晓栋），第六篇（左晓栋、孙锐），第七篇（耿玉波），第八篇（左晓栋），第九篇（高卓），第十篇（刘京京），第十一篇（郑立刚），第十二篇（朱良、高卓），第十三篇（朱良、高卓），第十四篇（朱良、高卓），第十五篇（高卓），第十六篇（高卓），第十七篇（高卓），第十八篇（高卓、孙锐），第十九篇（左晓栋），第二十篇（左晓栋），第二十一篇（左晓栋），第二十二篇（周亚超），第二十三篇（刘雨桁），第二十四篇（左晓栋），第二十五篇（王石），第二十六篇（刘雨桁），第二十七篇（周亚超），第二十八篇（张弛、崔占华、周亚超），第二十九篇（左晓栋），第三十篇（崔占华），第三十一篇（王石、刘雨桁、张弛），第三十二篇（崔占华），第三十三篇（左晓栋），第三十四篇（左晓栋），第三十五篇（周亚超），第三十六篇（刘雨桁、周亚超）；附录 I（刘雨桁），附录 II 由左晓栋整理。全书由左晓栋校对。

上海社会科学院互联网研究中心副主任方师师博士及其同事制作了书中各行业网络安全战略中文全文的二维码，并编辑了电子版、提供了发布平台。

本书篇幅较大，且美国的各项政策文件没有统一的格式，在电子工业出版社刘九如副社长的关心下，齐岳、苏颖杰两位编辑为此付出了艰辛努力，使本书得以高质量顺利出版。

感谢以上所有人员！

左晓栋

2017 年 12 月

## 反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036